

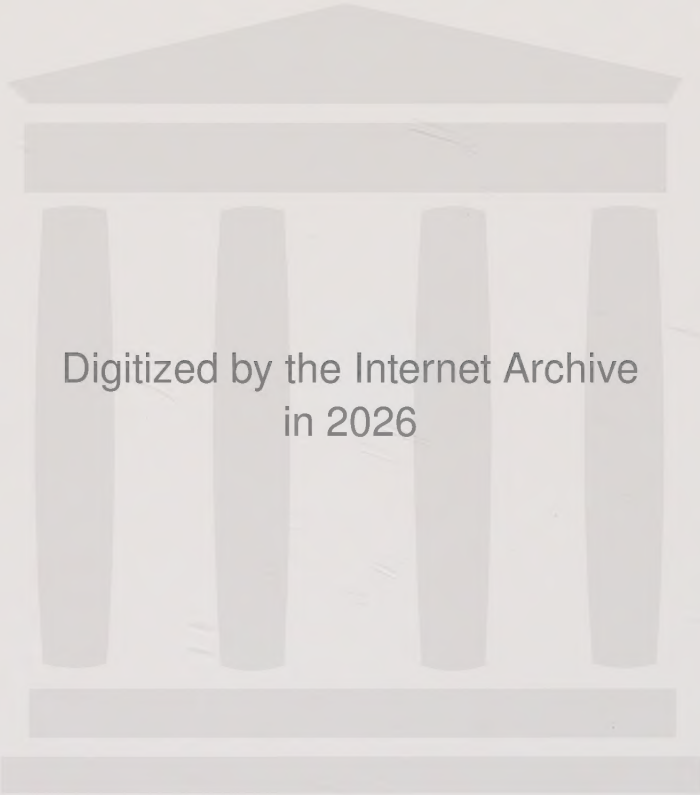
DER VIER-QUADRATE-SATZ
UND
EIN PROBLEM VON ERDÖS UND NATHANSON

D i s s e r t a t i o n
Zur Erlangung des Grades
„Doktor
der Naturwissenschaften“
am Fachbereich Mathematik
der Johannes Gutenberg-Universität
in Mainz

JOACHIM ZÖLLNER
geb. in Radeberg

Mainz ~~1984~~

1985



Digitized by the Internet Archive
in 2026

DER VIER-QUADRATE-SATZ
UND
EIN PROBLEM VON ERDÖS UND NATHANSON

D i s s e r t a t i o n
Zur Erlangung des Grades
"Doktor
der Naturwissenschaften"
am Fachbereich Mathematik
der Johannes Gutenberg-Universität
in Mainz

Joachim Zöllner
geb. in Radeberg

Mainz 1984

Erster Berichterstatter: Prof. Dr. G. Hofmeister

Zweiter Berichterstatter: Prof. Dr. E. Härtter

Tag der mündlichen Prüfung: 11. Februar 1985

Inhaltsverzeichnis

Einleitung		Seite 1
§ 1	Bezeichnungen und Vereinbarungen	6
§ 2	Bestimmung der unverzichtbaren Elemente in der Menge der Quadratzahlen als Basis der Ordnung vier	8
§ 3	"Dünne" Basen, die nur aus Quadraten bestehen	25
3.1	Hauptergebnisse dieses Paragraphen (Satz 4 und Satz 5)	25
3.2	Hilfsmittel aus der Wahrscheinlichkeitstheorie	26
3.3	Bezeichnungen für Darstellungsanzahlen	29
3.4	Anwendung der wahrscheinlichkeitstheoretischen Methode zur Herleitung von Satz 8	31
3.5	Einige Lemmata über Darstellungsanzahlen und Anzahlfunktionen	44
3.6	Abschätzungen der Darstellungsanzahlen spezieller quadratischer Formen	54
3.7	Beweis der Sätze 4 und 5	63
3.8	Anwendung der Ergebnisse auf Abschnittsbasen	71
3.9	Bemerkung zu möglichen Grenzen der hier verwendeten Beweismethode	72
3.10	Asymptotisches Verhalten der Anzahlfunktionen der in Satz 4 auftretenden Basen	73
Anhang:	Bemerkungen zu Basenkonstruktionen von Stöhr	78
	Basen, die auf Zifferndarstellungen beruhen	78
	Rekurrente Basen	81
Zusammenfassung		88
Literaturverzeichnis		89

Einleitung

Nach einem bekannten Satz von Lagrange ist jede natürliche Zahl darstellbar als Summe von vier Quadraten ganzer Zahlen. G. Hofmeister stellte 1973 die Frage, ob zu dieser Art von Darstellungen alle Quadrate benötigt werden oder nicht. Beispielsweise kann auf die Quadratzahl 25 nicht verzichtet werden, da in jeder Darstellung von 79 als Summe von vier Quadraten der Summand 25 auftritt: $79 = 49 + 25 + 4 + 1 = 36 + 25 + 9 + 9 = 25 + 25 + 25 + 4$. Als kleinstes Quadrat, auf welches man in dem genannten Sinn eventuell verzichten kann, kam 49 in Betracht, was 1974 in [24] auch bestätigt wurde. Darüber hinaus gibt es unendliche Mengen S von Quadraten, so daß jede natürliche Zahl als Summe von vier Quadraten, die nicht aus S sind, dargestellt werden kann. Kurz zuvor hatte E. Härtter eine entsprechende Aussage bezüglich der Darstellung als Differenz zweier Quadrate bewiesen, indem er zeigte, daß es unendliche Mengen T von Quadraten gibt, so daß jede natürliche Zahl $n \not\equiv 2 \pmod{4}$ Differenz von zwei Quadraten ist, die nicht aus T sind. Beide Ergebnisse findet man in [11].

In der additiven Zahlentheorie bezeichnet man eine Menge B von nicht-negativen ganzen Zahlen als Basis der Ordnung h , wenn sich jede natürliche Zahl als Summe von h Summanden aus B darstellen läßt. Beispielsweise bildet die Menge Q_0 der Quadrate aller nicht-negativen ganzen Zahlen eine Basis der Ordnung 4. Eine Quadratzahl $n^2 \in Q_0$ heißt verzichtbar, falls $Q_0 \setminus \{n^2\}$ Basis der Ordnung 4 ist, andernfalls unverzichtbar.

E. Deinert hatte 1977 auf der Grundlage umfangreicher numerischer Rechnungen vermutet, daß 0^2 , 5^2 , $(2^k)^2$ und $(3 \cdot 2^k)^2$, wobei k alle nicht-negativen ganzen Zahlen durchläuft, sämtliche unverzichtbaren Quadrate sind, was in [3] auch bewiesen wurde. Er bestimmte überdies zu je-

dem, dieser unverzichtbaren Quadrate n^2 die Menge $E(n^2)$ aller natürlichen Zahlen, zu deren Darstellung als Summe von vier beliebigen Quadraten die Zahl n^2 erforderlich ist, nachdem G. Pall [14] 1933 bereits $E(0^2)$ berechnet hatte. Entsprechende Charakterisierungen gelangen Härtter auch im Falle der Darstellung als Differenz von zwei Quadraten (siehe ebenfalls [3]).

Für eine Menge B von ganzen Zahlen und für jede positive reelle Zahl x sei

$$B(x) := \sum_{\substack{b \in B \\ 1 \leq b \leq x}} 1$$

die Anzahlfunktion von B . Die in [11] konstruierten Basen $Q_0 \setminus S$ der Ordnung 4 unterscheiden sich nur unwesentlich von Q_0 , obwohl $S \subseteq Q_0$ unendlich ist. Es gilt

$$\lim_{x \rightarrow \infty} \frac{(Q_0 \setminus S)(x)}{Q_0(x)} = 1.$$

Einen wesentlichen Fortschritt erzielten P. Erdős und M.B. Nathanson [7] 1981, indem sie zeigten, daß es zu jedem $\varepsilon > 0$ eine Basis B_ε der Ordnung 4 gibt, die nur aus Quadraten besteht, so daß mit einer Konstanten $C_\varepsilon > 0$ für alle natürlichen Zahlen n gilt

$$B_\varepsilon(n) \leq C_\varepsilon n^{3/8 + \varepsilon}.$$

Kurz darauf konnte Nathanson [13] den Exponenten auf $1/3 + \varepsilon$ verbessern. Erdős und Nathanson vermuteten in [7], daß $1/4 + \varepsilon$ erreichbar ist.

Die Beweise in den beiden letztgenannten Arbeiten verwenden Ergebnisse der Maßtheorie. In der Zahlentheorie wurde dieser Weg erstmals 1956 von Erdős [5] eingeschlagen und 1960 von Erdős und Rényi [8] systematisch ausgebaut. Da es sich bei den betrachteten Maßräumen um Wahrscheinlichkeitsräume handelt, spricht man bisweilen in der Zahlentheorie diesbezüglich von der "wahrscheinlichkeitstheoretischen Methode". Außer den genannten Ergebnissen konnten Erdős, Nathanson und andere eine Reihe von zahlentheoretischen Sätzen mit dieser Methode

erstmalig herleiten (z.B. [6]), welche z.T. bisher auf keinem anderen Weg bewiesen werden konnten.

In der endlichen additiven Zahlentheorie werden u.a. sogenannte Abschnittsbasen betrachtet. Sind h und n natürliche Zahlen, so heißt eine endliche Menge A nicht-negativer ganzer Zahlen Abschnittsbasis der Ordnung h für n , falls sich jede natürliche Zahl im Intervall $[1, n]$ als Summe von h Summanden aus A darstellen läßt. S.L.G. Choi, P. Erdős und M.B. Nathanson [2] zeigten 1980 auf konstruktivem Wege, daß es für jedes $n \geq 2$ eine Abschnittsbasis A der Ordnung 4 gibt, die nur aus Quadraten besteht, für welche gilt

$$|A| \leq \frac{4}{\log 2} n^{1/3} \log n .$$

Auch hier wurde vermutet, daß es zu jedem $\varepsilon > 0$ und für jedes in Abhängigkeit von ε genügend große n eine Abschnittsbasis A_ε der Ordnung 4 gibt, so daß gilt

$$|A_\varepsilon| \leq n^{1/4 + \varepsilon} .$$

In diesem Zusammenhang ist eine Untersuchung von E.S. Selmer [17] interessant, der für Mengen $Q_0 \cap [0, k^2]$ der ersten $k+1$ aufeinanderfolgenden Quadrate die maximale Zahl n bestimmte, so daß $Q_0 \cap [0, k^2]$ Abschnittsbasis der Ordnung 4 für n ist.

In der vorliegenden Arbeit wird - im Anschluß an § 1, der einige Bezeichnungen und sonstige Vorbereitungen enthält - in § 2 gezeigt, daß die von E. Deinert angegebenen Quadrate $0^2, 5^2, (2^k)^2$ und $(3 \cdot 2^k)^2$ ($k \geq 0$) tatsächlich sämtliche unverzichtbaren Quadrate sind. Das in diesem Zusammenhang wichtige Lemma 1 stammt von Deinert, sowie die Einführung der zuvor erwähnten Menge $E(n^2)$. Auf Deinert gehen auch einige Vereinfachungen in den Tabellen des Beweises von Lemma 6, sowie die Berechnung der Tabelle zum Fall 3 dieses Beweises zurück. Einen Teil der Aussage von Lemma 7 hatte er zuvor in anderer Weise mit Hilfe zahlreicher Darstellungsformeln zeigen können.

In § 3, dem Hauptteil, werden die erwähnten Vermutungen von Erdős und Nathanson, sowie von Choi, Erdős und Nathanson mit Hilfe der maßtheoretischen Methode von Erdős und Rényi bewiesen. Allgemeiner wird gezeigt, daß es zu jedem $h \geq 4$ und jedem $\varepsilon > 0$ eine Basis $B_{h,\varepsilon}$ und eine Abschnittsbasis $A_{h,\varepsilon}$ für n gibt, die beide nur aus Quadraten bestehen, so daß für eine Konstante $C(h,\varepsilon) > 0$ gilt

$$B_{h,\varepsilon}(n) \leq C(h,\varepsilon)n^{1/h+\varepsilon} \text{ für alle } n$$

und

$$|A_{h,\varepsilon}| \leq n^{1/h+\varepsilon} \text{ für alle genügend großen } n.$$

Die Aussage über Abschnittsbasen folgt dabei in einfacher Weise aus dem Ergebnis über Basen.

Durch die Beweismethode bedingt, wird für diese Basen und Abschnittsbasen kein konstruktives Verfahren geliefert, sondern nur deren Existenz bewiesen. Außerdem ist die Konstante $C(h,\varepsilon)$ nicht effektiv berechenbar. Es lassen sich aber Angaben über das asymptotische Verhalten von $B_{h,\varepsilon}(n)$ machen, die den Abschluß von § 3 bilden.

Wichtigster Ausgangspunkt für die Beweise in § 3 ist ein Lemma von Erdős und Nathanson [7], daß hier als Lemma 10 angeführt wird. Auch in die Beweise der Lemmata 15 und 23 fließen Anregungen aus der genannten Arbeit ein.

Im Anhang der vorliegenden Arbeit finden sich noch einige Bemerkungen zu den von A. Stöhr [21] konstruierten Basen, die auf Zifferndarstellungen beruhen, sowie zu einem Problem von Stöhr [23], die von ihm eingeführten rekurrenten Basen betreffend.

Herrn G. Hofmeister, der (soweit mir bekannt ist) als erster auf den hier behandelten Problemkreis aufmerksam gemacht hat, und Herrn E. Härtter gilt mein besonderer Dank, ohne deren vielfältige Unterstützung diese Arbeit nicht begonnen worden wäre; ferner Herrn E. Deinert

für die erwähnte Zusammenarbeit in § 2, sowie den Teilnehmern am Oberseminar Additive Zahlentheorie SS 1984 in Mainz für die kritische Diskussion von § 3 im Rahmen einer Vortragsreihe.

§ 1 Bezeichnungen und Vereinbarungen

Für beliebige Mengen M bezeichne $|M|$ die Kardinalzahl von M .

Sei $\mathbb{N} = \{1, 2, \dots\}$ die Menge der natürlichen Zahlen und sei $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

$\mathbb{Z}$ bezeichne die Menge der ganzen und $\mathbb{R}$ die Menge der reellen Zahlen.

Ist $x \in \mathbb{R}$, so sei $[x]$ die größte ganze Zahl $\leq x$ und $\langle x \rangle$ die kleinste ganze Zahl $\geq x$.

Leere Summen sind 0 und leere Produkte sind 1 zu setzen.

Für $h \in \mathbb{N}_0$ und $A_i \subseteq \mathbb{N}_0$, $i=1, 2, \dots, h$ sei

$$A_1 + A_2 + \dots + A_h = \sum_{i=1}^n A_i := \{a^{(1)} + a^{(2)} + \dots + a^{(h)} \mid a^{(i)} \in A_i\}.$$

Ist $A \subseteq \mathbb{N}_0$, so bedeute

$$hA := \sum_{i=1}^n A, \quad 1A := A, \quad 0A := 0.$$

und

$$h \circ A := \bigcup_{j=1}^n jA.$$

Gilt für $M \subseteq \mathbb{N}_0$, daß $M \subseteq hA$ ist, so heißt A Basis der Ordnung h für M . Ist $M = \mathbb{N}$, dann heißt A Basis der Ordnung h , oder nur Basis, wenn es auf den Wert von h nicht ankommt.

Sei

$$n = a^{(1)} + a^{(2)} + \dots + a^{(h)}, \quad a^{(i)} \in A, \quad i=1, 2, \dots, h.$$

Falls keine Verwechslungen zu befürchten sind, verwenden wir $a^{(1)} + a^{(2)} + \dots + a^{(h)}$ sowohl in der Bedeutung als Zahl, in diesem Falle also n , wie auch in der Bedeutung

als Darstellung, d.h. genauer als Darstellungstupel $(a^{(1)}, a^{(2)}, \dots, a^{(h)})$ der Zahl n durch h Summanden aus A . Unterscheiden sich zwei verschiedene Darstellungen von n nicht nur in der Reihenfolge ihrer Summanden (genauer: ihrer Komponenten), so heißen sie wesentlich verschieden.

Für $A \subseteq \mathbb{N}_0$ und $x \in \mathbb{R}$ sei

$$A(x) := \sum_{\substack{a \in A \\ 1 \leq a \leq x}} 1.$$

$A(x)$ heißt Anzahlfunktion von A .

Seien $a, b \in \mathbb{R}$ und $s: [a, +\infty[\rightarrow \mathbb{R}$, $t: [b, +\infty[\rightarrow \mathbb{R}$ zwei Funktionen. Existiert der folgende Grenzwert und gilt

$$\lim_{x \rightarrow +\infty} \frac{s(x)}{t(x)} = 1,$$

so schreibt man

$$s(x) \sim t(x).$$

Die beiden Funktionen bezeichnet man dann als asymptotisch gleich.

Mit Q bezeichnen wir die Menge der Quadrate der natürlichen Zahlen. Ferner sei $Q_0 := Q \cup \{0\}$.

§ 2 Bestimmung der unverzichtbaren Elemente
in der Menge der Quadratzahlen als Basis der Ordnung vier

In diesem Paragraphen wird folgender Satz bewiesen:

Satz 1. Sei $n \in \mathbb{N}_0$. Es gilt:

$$a) 4(Q_0 \setminus \{n^2\}) = \mathbb{N}_0 \Leftrightarrow n \notin \{0, 5, 2^m, 3 \cdot 2^m \mid m \in \mathbb{N}_0\}.$$

D.h.: Genau dann ist jedes $z \in \mathbb{N}_0$ darstellbar als Summe von 4 Quadraten, die von n^2 verschieden sind, wenn $n \notin \{0, 5, 2^m, 3 \cdot 2^m \mid m \in \mathbb{N}_0\}$.

$$b) 4(Q_0 \setminus \{n^2\}) \sim \mathbb{N}_0 \Leftrightarrow n \neq 0. \text{ D.h.:}$$

Genau dann ist jedes genügend große $z \in \mathbb{N}_0$ darstellbar als Summe von 4 Quadraten, die von n^2 verschieden sind, wenn $n \neq 0$ ist.

Zum Beweis von Satz 1 benötigen wir noch einige weitere Bezeichnungen und Hilfsmittel.

Für jedes $n \in \mathbb{N}_0$ sei $E(n^2)$ die Menge aller $z \in \mathbb{N}_0$, für die gilt:

Aus $z = a_1^2 + a_2^2 + a_3^2 + a_4^2$ mit $a_i \in \mathbb{N}_0$ ($i=1,2,3,4$) folgt $a_i^2 = n^2$ für mindestens ein i .

In $E(n^2)$ sind also alle Zahlen $z \in \mathbb{N}_0$ zusammengefaßt, zu deren Darstellung als Summe von 4 Quadraten n^2 erforderlich ist.

Es sei weiter

$$U := \{n^2 \mid n \in \mathbb{N}_0, E(n^2) \neq \emptyset\}$$

die Menge der unverzichtbaren Quadrate und

$$\tilde{U} := \{n^2 \mid n \in \mathbb{N}_0, |E(n^2)| = \infty\}$$

die Menge der asymptotisch unverzichtbaren Quadrate in Q_0 .

Ferner sei

$$V := Q_0 \setminus U$$

die Menge der verzichtbaren Quadrate und

$$\tilde{V} := Q_0 \setminus \tilde{U}$$

die Menge der asymptotisch verzichtbaren Quadrate in Q_0 .

Damit läßt sich Satz 1 auch kurz folgendermaßen formulieren:

Satz 1'. $U = \{n^2 \mid n = 0, 5, 2^m, 3 \cdot 2^m \text{ mit } m \in \mathbb{N}_0\}$

und

$$\tilde{U} = \{0^2\}.$$

Daher ist 7^2 das kleinste Element von V ; außerdem gilt $\tilde{V} = Q$.

Satz 1 werden wir in der Formulierung von Satz 1' beweisen.

Es gilt folgender bekannter

Satz 2. $n \in \mathbb{N}_0$ ist genau dann als Summe von 3 Quadraten aus Q_0 darstellbar, wenn $n \neq 4^a(8b+7)$ für alle $a, b \in \mathbb{N}_0$ gilt. ¹⁾

¹⁾ Siehe etwa Landau [12], S. 122-123.

Wir zeigen weiter

Lemma 1 (Deinert²⁾). Sei $z \in \mathbb{N}$, $4|z$ und $n^2 \in \mathbb{Q}_0$, so gilt:
 $z \in E(n^2)$ genau dann, wenn $8|z$, $2|n$ und $\frac{z}{4} \in E((\frac{n}{2})^2)$.

Beweis. Sei zuerst $z \in E(n^2)$. Wegen $4|z$ gibt es Zahlen $a_i \in \mathbb{N}_0$, $i=1,2,3,4$, mit

$$\frac{z}{4} = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Also ist

$$(1) \quad z = (2a_1)^2 + (2a_2)^2 + (2a_3)^2 + (2a_4)^2.$$

Wegen $z \in E(n^2)$ folgt $2a_i = n$ für ein $i \in \{1,2,3,4\}$, also $2|n$ und $a_i = \frac{n}{2}$ für dieses i . Damit ist $\frac{z}{4} \in E((\frac{n}{2})^2)$.

Wir nehmen nun an $8 \nmid z$. Da $4|z$, folgt $z-1 \equiv 3 \pmod{8}$.

Nach Satz 2 ist dann

$$z-1 = b_1^2 + b_2^2 + b_3^2$$

für gewisse $b_1, b_2, b_3 \in \mathbb{N}_0$.

Aus $z-1 \equiv 3 \pmod{8}$ folgt auch, daß b_1, b_2 und b_3 ungerade sein müssen. Also ist

$$z = b_1^2 + b_2^2 + b_3^2 + 1^2$$

und jedes der vier Quadrate ist ungerade und daher ungleich n^2 . Das widerspricht $z \in E(n^2)$. Also gilt $8|z$.

Sei nun umgekehrt $8|z$, $2|n$ und $\frac{z}{4} \in E((\frac{n}{2})^2)$. Wegen $8|z$ hat z nur Darstellungen der Form (1). Damit ist $\frac{z}{4} = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Aus $\frac{z}{4} \in E((\frac{n}{2})^2)$ folgt nun $z \in E(n^2)$ ■

2) siehe [3].

Für $n \in \mathbb{N}_0$ sei X_n die Menge aller $x \in \mathbb{N}_0$, für die gilt:

$$(2) \quad \begin{aligned} n^2 + x^2 &= a_1^2 + a_2^2 \\ 2n^2 + x^2 &= b_1^2 + b_2^2 + b_3^2 \\ 3n^2 + x^2 &= c_1^2 + c_2^2 + c_3^2 + c_4^2 \end{aligned}$$

mit $a_i, b_j, c_k \in \mathbb{N}_0 \setminus \{n\}$.

Für die drei Gleichungen (2) schreiben wir bei gegebenem $n \in \mathbb{N}_0$ und $x \in \mathbb{N}_0$ abkürzungsweise auch

$$\begin{aligned} &(a_1, a_2) \\ &(b_1, b_2, b_3) \\ &(c_1, c_2, c_3, c_4) \end{aligned} .$$

Lemma 2. Sei $n^2 \in Q_0$. Existiert zu $x \in X_n$, $x \neq n$ ein $z \in \mathbb{N}_0$, $z > x^2$ so, daß $z - x^2$ als Summe von drei Quadraten aus Q_0 darstellbar ist, so gilt $z \notin E(n^2)$.

Beweis. Es gilt also

$$\begin{aligned} z &= x^2 + x_1^2 + x_2^2 + x_3^2 \\ &\text{für gewisse } x_i \in \mathbb{N}_0, i=1,2,3 . \end{aligned}$$

Ist $x_i \neq n$ für $i=1,2,3$, so haben wir eine Darstellung von z ohne n^2 als Summanden.

Für die übrigen Fälle erhalten wir nach Definition von X_n die folgenden neuen Darstellungen von z , in denen n^2 nicht als Summand auftritt:

$$\begin{aligned} x_1 &= n, \quad x_2 \neq n + x_3; & z &= x^2 + n^2 + x_2^2 + x_3^2 = a_1^2 + a_2^2 + x_2^2 + x_3^2 ; \\ x_1 &= x_2 = n, \quad x_3 \neq n; & z &= x^2 + 2n^2 + x_3^2 = b_1^2 + b_2^2 + b_3^2 + x_3^2 ; \\ x_1 &= x_2 = x_3 = n; & z &= x^2 + 3n^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2 . \end{aligned}$$

Also ist $z \notin E(n^2)$. Damit ist Lemma 2 bewiesen ■

Für $d, z \in \mathbb{N}$ sei

$$w^{(d)}(z) := |\{(x, y) \in \mathbb{N}_0 \mid x^2 + dy^2 = z\}| ,$$

also die Anzahl der wesentlich verschiedenen Darstellungen von z durch die Form $x^2 + dy^2$.

Lemma 3. Sei $d \in \{1, 2\}$ und $z \in \mathbb{N}$.

Falls $x_1, x_2 \in \mathbb{N}_0$ existieren mit

$$x_1^2 + dx_2^2 = z,$$

dann gilt:

a) $w^{(1)}(z) \geq 2$ genau dann, wenn z mindestens zwei (nicht notwendig verschiedene) Primfaktoren $\equiv 1 \pmod{4}$ besitzt.

b) Seien $p_1, p_2, \dots, p_r$ die sämtlichen Primfaktoren $\equiv 1$ oder $3 \pmod{8}$ von z (wobei auch gleiche zugelassen sind), dann gilt:

$w^{(2)}(z) \geq 3$ genau dann, wenn $\begin{cases} r \geq 4, & \text{falls } p_1 = p_2 = \dots = p_r \\ r \geq 3 & \text{sonst.} \end{cases}$

Beweis. Wegen der Existenz wenigstens einer Darstellung $z = x_1^2 + dx_2^2$ ist $w^{(d)}(z) \geq 1$ für $d=1, 2$.

Es sei p eine Primzahl, dann werde für $z \in \mathbb{N}$ die Zahl

$$e_p(z) \in \mathbb{N}_0$$

definiert durch $p^{e_p(z)} \mid z$ und $p^{e_p(z)+1} \nmid z$.

a) Für die Anzahl $r(z)$ aller Darstellungen von z durch die Form $x^2 + y^2$ mit $x, y \in \mathbb{Z}$ gilt bekanntlich (siehe etwa Hardy und Wright [10], S. 241, Satz 278):

$$r(z) = 4 \prod_{\substack{p \mid z \\ p \text{ Primz.} \\ p \equiv 1 \pmod{4}}} (1 + e_p(z)),$$

denn wegen $w^{(1)}(z) \geq 1$ ist $r(z) \geq 1$.

Es kann $z \in \mathbb{N}$ höchstens eine der beiden wesentlich verschiedenen Darstellungen $z = x_1^2 + x_1^2$ bzw. $z = x_2^2 + 0^2$ be-

sitzen. Zu jeder dieser Darstellungen gibt es genau vier Darstellungen durch Quadrate ganzer Zahlen mit Berücksichtigung der Summandenreihenfolge, nämlich

$$\begin{array}{ccc} x_1^2 + x_1^2 & & x_2^2 + 0^2 \\ x_1^2 + (-x_1)^2 & & (-x_2)^2 + 0^2 \\ (-x_1)^2 + x_1^2 & \text{bzw.} & 0^2 + x_2^2 \\ (-x_1)^2 + (-x_1)^2 & & 0^2 + (-x_2)^2 \end{array} .$$

Zu jeder anderen wesentlich verschiedenen Darstellung

$$z = x^2 + y^2$$

gibt es genau acht Darstellungen, nämlich

$$(\pm x)^2 + (\pm y)^2, (\pm y)^2 + (\pm x)^2 .$$

Es folgt

$$w^{(1)}(z) = \frac{r(z) - 4}{8} + 1 \quad \text{oder} \quad w^{(1)}(z) = \frac{r(z)}{8} .$$

Ist $w^{(1)}(z) \geq 2$, so gilt

$$2 \leq w^{(1)}(z) \leq \frac{r(z) - 4}{8} + 1$$

$$3 \leq \frac{r(z)}{4} = \prod_{\substack{p|z \\ p \text{ Primz.} \\ p \equiv 1 \pmod{4}}} (1 + e_p(z)) .$$

Also besitzt z wenigstens zwei Primfaktoren $\equiv 1 \pmod{4}$.

Wenn umgekehrt dies zutrifft, so folgt

$$3 \leq \frac{r(z)}{4} \leq 2 w^{(1)}(z) ,$$

also $w^{(1)}(z) \geq 2$, da $w^{(1)}(z) \in \mathbb{Z}$.

b) Die Anzahl $r^{(2)}(z)$ aller Darstellungen von z durch die Form $x^2 + 2y^2$ mit $x, y \in \mathbb{Z}$ ist nach Dickson [4],

S. 80 gegeben durch

$$r^{(2)}(z) = 2 \sum_{t|z} \chi(t) \quad \text{mit} \quad \chi(t) := \begin{cases} 0 & \text{für } t \equiv 0 \pmod{2} \\ 1 & \text{für } t \equiv 1 \text{ od. } 3 \pmod{8} \\ -1 & \text{für } t \equiv 5 \text{ od. } 7 \pmod{8} . \end{cases}$$

Es folgt

$$\begin{aligned} r^{(2)}(z) &= 2 \prod_{\substack{p|z \\ p \text{ Primz.}}} (\chi(1) + \chi(p) + \dots + \chi(p^{e_p(z)})) \\ &= 2 \prod_{\substack{p|z \\ p \text{ Primz.} \\ p \equiv 1 \text{ od. } 3 \pmod{8}}} (1 + e_p(z)) \quad , \text{ da } r^{(2)}(z) > 1. \end{aligned}$$

Da z höchstens eine der beiden wesentlich verschiedenen Darstellungen $z = x_1^2 + 2 \cdot 0^2$ bzw. $z = 0^2 + 2x_2^2$ besitzen kann, denen jeweils zwei Darstellungen mit Quadraten ganzer Zahlen zugeordnet sind, während jeder anderen wesentlich verschiedenen Darstellung deren vier zugeordnet sind, so folgt

$$w^{(2)}(z) = \frac{r^{(2)}(z) - 2}{4} + 1 \quad \text{oder} \quad w^{(2)}(z) = \frac{r^{(2)}(z)}{4}.$$

Ist $w^{(2)}(z) > 3$, so gilt

$$\begin{aligned} 3 &< w^{(2)}(z) < \frac{r^{(2)}(z) - 2}{4} + 1 \\ 5 &< \frac{r^{(2)}(z)}{2} = \prod_{\substack{p|z \\ p \text{ Primz.} \\ p \equiv 1 \text{ od. } 3 \pmod{8}}} (1 + e_p(z)). \end{aligned}$$

Also besitzt z wenigstens drei Primfaktoren $\equiv 1 \text{ oder } 3 \pmod{8}$ und sogar vier, falls alle gleich sind.

Umgekehrt folgt daraus

$$5 < \frac{r^{(2)}(z)}{2} < 2 w^{(2)}(z),$$

also $w^{(2)}(z) > 3$ ■

Lemma 4. Sei $0 \neq z = x^2 + y^2$ mit $x, y \in \mathbb{N}_0$ und $2 \nmid x$ oder $2 \nmid y$. Es gelte ferner

(i) $p^2 \nmid z$ für eine Primzahl $p \equiv 1 \pmod{4}$ oder

(ii) $5 \nmid z$, $z > 10$ und aus $p \mid \text{ggT}(x, y)$, p prim folgt $p \equiv 1 \pmod{4}$.

Dann ist $w^{(1)}(z) \geq 2$.

Beweis. Gilt (i), so erhält man die Behauptung aus Lemma 3, Teil a).

Es gelte nun (ii). Sei $p|z$ für eine ungerade Primzahl p .

Gilt $p \nmid y$, so ist wegen $p|z$ die Kongruenz

$$x^2 + y^2 \equiv 0 \pmod{p}$$

in x lösbar. Es folgt

$$1 = \left(\frac{-y^2}{p} \right) = \left(\frac{-1}{p} \right).$$

Also ist $p \equiv 1 \pmod{4}$.

Ist aber $p|y$, dann folgt $p|z - y^2 = x^2$, also $p|ggT(x,y)$.

Damit gilt ebenfalls $p \equiv 1 \pmod{4}$ nach Voraussetzung.

Die ungeraden Primfaktoren von z sind also alle $\equiv 1 \pmod{4}$.

Wegen $2 \nmid x$ oder $2 \nmid y$ tritt der Faktor 2 höchstens einmal

auf. Da $\frac{z}{5} > 2$, besitzt $\frac{z}{5}$ mindestens einen Primfaktor

$\equiv 1 \pmod{4}$, also z mindestens deren zwei. Aus Lemma 3,

Teil a) folgt $w^{(1)}(z) \geq 2$.

Lemma 5. Sei $0 \neq z = x^2 + 2y^2$ mit $x, y \in \mathbb{N}_0$ und $2 \nmid x$ oder $2 \nmid y$,

sowie $9|z$, $z > 54$ und für jede Primzahl p mit

$p|ggT(x,y)$ gelte $p \equiv 1$ oder $3 \pmod{8}$.

Dann ist $w^{(2)}(z) \geq 3$.

Beweis. Analog zum Beweis von Lemma 4 folgt, daß z nur

Primfaktoren $\equiv 1$ oder $3 \pmod{8}$ und höchstens einmal den

Faktor 2 enthält.

Wegen $\frac{z}{9} > 6$ enthält $\frac{z}{9}$ mindestens einen Primfaktor $p' \equiv 1$ oder

$3 \pmod{8}$. Sind alle ungeraden Primfaktoren von $\frac{z}{9}$ gleich 3,

dann folgt aus $\frac{z}{9} > 3 \cdot 2$, daß $3^2 | \frac{z}{9}$, also $3^4 | z$. Andernfalls be-

sitzt z wegen $9p'|z$ mindestens drei ungerade Primfaktoren,

die nicht alle gleich sind. Mit Lemma, Teil b) erhalten wir in beiden Fällen $w^{(2)}(z) \geq 3$ ■

Lemma 6. Sei t ungerade, $t \neq 9$ oder sei $t = 10$ oder 18 .

Dann gibt es in X_t eine gerade Zahl $x_g \neq t$ und eine ungerade Zahl $x_u \neq t$.

Im Falle $t > 5$ kann man $x_g < t$ und $x_u < t$ wählen.

Beweis.

1. Fall: Sei t ungerade, $t > 5$ und es existiert eine Primzahl $p|t$ mit $p \equiv 1 \pmod{4}$.

Man setze für	$t^2 \equiv$	0	1	4	(mod 5)
	$x_u =$	5	13	1	
	$x_g =$	10	2	4	

Die folgenden Aussagen im Fall 1 gelten für jedes $x \in \{x_u, x_g\}$.

Für $z := t^2 + x^2$ sind dann die Bedingungen von Lemma 4 (ii)

erfüllt, und es gilt $w^{(1)}(z) \geq 2$. Also existiert eine

weitere Darstellung $z = a^2 + b^2$, $a, b \in \mathbb{N}_0$ mit $a \neq t \neq b$. Der

kleinstmögliche Wert für t in diesem Fall ist 13, und

es gilt $t^2 \equiv 13^2 \equiv 4 \pmod{5}$. Aus obiger Tabelle entnimmt

man nun sofort, daß für alle zulässigen t gilt $x < t$.

Wegen $p^2 | 2t^2$ erhält man aus Lemma 3, Teil a), daß

$w^{(1)}(2t^2) \geq 2$. Damit ist $2t^2 = c^2 + d^2$ für gewisse $c, d \in \mathbb{N}_0$

mit $c \neq t \neq d$. Wir haben gezeigt

$$t^2 + x^2 = a^2 + b^2$$

$$2t^2 + x^2 = c^2 + d^2 + x^2$$

$$3t^2 + x^2 = a^2 + b^2 + c^2 + d^2,$$

wobei alle Quadrate auf den rechten Seiten dieser Gleichungen von t^2 verschieden sind. Also gilt $x_g, x_u \in X_t$ und

$x_g < t$, $x_u < t$.

2. Fall: Sei t ungerade und für alle Primfaktoren p von t gelte $p \equiv 3 \pmod{4}$, und darüber hinaus sei $t \neq 1, 3, 7, 11, 19, 23, 27, 31, 33, 49$ und 59 .

Man setze für

$t^2 \equiv$	0	1	4	7 (mod 9)
(3) 1 (mod 5)	$(x_u, x_g) = (3, 12) (13, 32) (17, 8) (97, 2)$			
4 (mod 5)	$(39, 6) (41, 4) (1, 26) (29, 16)$			

Falls $t > 97$, ist $x_u < t$ und $x_g < t$. Auch für die übrigen in diesem Fall betrachteten Werte von t trifft das zu, wie man aus (3) entnehmen kann. Dort erhält man für

$$t = 21 \ 43 \ 47 \ 57 \ 63 \ 67 \ 69 \ 71 \ 77 \ 79 \ 81 \ 83 \ 97$$

$$x_u = 3 \ 1 \ 1 \ 39 \ 39 \ 29 \ 3 \ 13 \ 29 \ 17 \ 3 \ 1 \ 39$$

$$x_g = 12 \ 26 \ 26 \ 6 \ 6 \ 16 \ 12 \ 32 \ 16 \ 8 \ 12 \ 26 \ 6 .$$

x_u und x_g sind so gewählt, daß sie als Primfaktoren höchstens einmal die 3 und des weiteren nur solche $\neq 3 \pmod{4}$ besitzen.

Es sei wieder x beliebig aus $\{x_u, x_g\}$ zugelassen.

Aus (3) folgt auch, daß in jedem Fall

$$t^2 + x^2 \equiv 0 \pmod{5} \quad \text{und} \quad 2t^2 + x^2 \equiv 0 \pmod{9}$$

gilt. Wegen $t > 11$ ist $121 < t^2 + x^2 < 2t^2 + x^2$. Für $3 \nmid \text{ggT}(t, x)$ ist die Bedingung (ii) von Lemma 4 für $z := t^2 + x^2$ erfüllt. Desgleichen für $\frac{z}{9}$, falls $3 \mid \text{ggT}(t, x)$, denn $10 < \frac{121}{9} < \frac{z}{9} = \left(\frac{t}{3}\right)^2 + \left(\frac{x}{3}\right)^2$, und wegen $3 \nmid \frac{x}{3}$ ist $3 \nmid \text{ggT}(\frac{t}{3}, \frac{x}{3})$. Es folgt $w^{(1)}(\frac{z}{9}) \geq 2$. Daher ist in beiden Fällen $w^{(1)}(z) \geq 2$. Also gibt es $a_1, a_2 \in \mathbb{N}_0$ mit $a_1 + t + a_2$ und

$$t^2 + x^2 = a_1^2 + a_2^2 .$$

Wir betrachten nun $z_1 := 2t^2 + x^2 \equiv 0 \pmod{9}$. Die Zahl t

hat nur Primfaktoren $\equiv 3 \pmod{4}$, so daß $\text{ggT}(t,x)=1$ oder 3 ist. Damit sind für z_1 die Voraussetzungen von Lemma 5 erfüllt, und es gilt $w^{(2)}(z_1) > 3$. Also existieren zwei weitere Darstellungen dieser Art von z_1 , die nicht beide t enthalten können. Es gibt also $b_1, b_2 \in \mathbb{N}_0$ mit $b_1 + t \neq b_2$ und

$$2t^2 + x^2 = b_1^2 + 2b_2^2.$$

Wegen $3t^2 + x_u^2 \equiv 4 \pmod{8}$ folgt aus Lemma 1, daß $3t^2 + x_u^2 \notin E(t^2)$. Es gibt also Zahlen $c_i \neq t$, $i=1,2,3,4$ mit

$$3t^2 + x_u^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2.$$

Damit ist $x_u \in X_t$ gezeigt.

Um auch $x_g \in X_t$ nachzuweisen, genügt es, $3t^2 + x_g^2 \notin E(t^2)$ zu zeigen.

Es gilt $z_2 := 3t^2 + x_g^2 \equiv 3 \pmod{4}$. Wir betrachten $z_2 - x_u^2 \equiv 2 \pmod{4}$. Nach Satz 2 besitzt $z_2 - x_u^2$ eine Darstellung als Summe von drei Quadraten. Wegen $z_2 - x_u^2 > t^2 - x_u^2 > 0$ folgt aus Lemma 2, daß $3t^2 + x_g^2 = z_2 \notin E(t^2)$.

3. Fall: $t = 1, 3, 5, 7, 11, 19, 23, 27, 31, 33, 49, 59, 10$ oder 18.

Hier geben wir $x_u, x_g \in X_t$ und die $a_i, b_j, c_k \in \mathbb{N}_0 \setminus \{t\}$ in (2) direkt an. Dabei gilt $x_u + t \neq x_g$, und für $t > 5$ ist $x_u < t$, $x_g < t$ erfüllt.

$t=1, x_u=13,$	(11,7)	$t=3, x_u=21,$	(15,15)
	(11,5,5)		(19,7,7)
	(10,6,6,0)		(21,5,1,1)
$x_g=8,$	(7,4)	$x_g=16,$	(12,11)
	(5,5,4)		(15,7,0)
	(7,3,3,0)		(16,5,1,1)

t=5, $x_u=15$, (13,9)	t=7, $x_u=1$, (5,5)
(15,7,1)	(9,3,3)
(17,3,1,1)	(12,2,0,0)
$x_g=0$, (4,3)	$x_g=4$, (8,1)
(7,1,0)	(8,5,5)
(8,3,1,1)	(12,3,3,1)
t=11, $x_u=3$, (9,7)	t=19, $x_u=3$, (17,9)
(15,5,1)	(27,1,1)
(19,3,1,1)	(32,8,2,0)
$x_g=2$, (10,5)	$x_g=2$, (14,13)
(14,5,5)	(26,7,1)
(19,2,1,1)	(31,11,2,1)
t=23, $x_u=1$, (19,13)	t=27, $x_u=1$, (21,17)
(31,7,7)	(37,9,3)
(39,7,3,3)	(46,8,2,2)
$x_g=2$, (22,7)	$x_g=4$, (24,13)
(31,10,1)	(36,13,3)
(39,6,5,3)	(45,13,3,0)
t=31, $x_u=1$, (29,11)	t=33, $x_u=1$, (27,19)
(43,7,5)	(37,27,9)
(53,7,5,1)	(57,3,3,1)
$x_g=2$, (26,17)	$x_g=4$, (32,9)
(42,9,9)	(45,13,0)
(53,7,5,2)	(57,5,3,0)
t=49, $x_u=3$, (41,27)	t=59, $x_u=3$, (49,33)
(69,7,1)	(83,9,1)
(83,17,5,3)	(102,4,4,4)
$x_g=2$, (47,14)	$x_g=2$, (58,11)
(69,6,3)	(82,11,11)
(83,17,5,2)	(99,23,9,6)

$t=10, x_u=5, (11,2)$	$t=18, x_u=1, (17,6)$
$(10,7,1)$	$(24,8,3)$
$(13,2,1,1)$	$(31,2,1,1)$
$x_g=0, (8,6)$	$x_g=4, (14,12)$
$(14,2,0)$	$(22,12,6)$
$(16,6,2,2)$	$(31,4,2,1) \blacksquare$

Lemma 7. Sei $t \in \mathbb{N}$, $4 \nmid t$ und $n = 2^r t$ mit $r \in \mathbb{N}_0$, sowie $z \in \mathbb{N}_0$.

Existieren $x_u, x_g \in X_t$ mit $2 \nmid x_u + t$ und $2 \mid x_g + t$,
so folgt aus

$$z > \max((2^r x_u)^2, (2^r x_g)^2),$$

daß $z \notin E(n^2)$.

Beweis. Für $z < n^2$ gilt trivialerweise $z \notin E(n^2)$. Sei also $z \geq n^2$.

1. Fall: $z - (2^r x_u)^2$ oder $z - (2^r x_g)^2$ ist als Summe dreier Quadrate darstellbar.

Für ein $x \in \{x_u, x_g\}$ sei dies zutreffend. Multipliziert man die Gleichungen (2) mit $(2^r)^2$, so erhält man, da $x \in X_t$,

$$2^r x \in X_{2^r t} = X_n.$$

Wegen $x_u + t \equiv x_g \pmod{2}$ ist $n = 2^r t \equiv 2^r x \pmod{2}$. Daher folgt aus Lemma 2, daß $z \notin E(n^2)$.

2. Fall: $z - (2^r x_u)^2$ und $z - (2^r x_g)^2$ sind nicht als Summen von drei Quadraten darstellbar.

Nach Satz 2 gilt dann mit gewissen $a, b, c, d \in \mathbb{N}_0$

$$(4) \quad z - (2^r x_u)^2 = 4^a (8b+7),$$

$$(5) \quad z - (2^r x_g)^2 = 4^c (8d+7).$$

Aus diesen Gleichungen folgt

$$(6) \quad 4^{r'} (x_g^2 - x_u^2)^2 = 4^{a'} (8b+7) - 4^{c'} (8d+7),$$

wobei wenigstens eine der Zahlen $r', a', c' \in \mathbb{N}_0$ gleich 0 sei.

Ist $r'=0$, so gilt

$$3 \equiv x_g^2 - x_u^2 = 4^{a'}(8b+7) - 4^{c'}(8d+7) \pmod{4}.$$

Damit ist $a'=0$ und $c' > 0$ und es gilt $a=r$. Aus (4) folgt wegen $x_u^2 \equiv 1 \pmod{8}$, daß

$$z' := \frac{z}{4^r} = 8b+7 + x_u^2 \equiv 0 \pmod{8}.$$

Sei $x_g = 2^m s$ mit $m \in \mathbb{N}$, $2 \nmid s \in \mathbb{N}$ oder $s=0$. Aus (5) folgt

$$(7) \quad z' = \frac{z}{4^r} = 4^{c'}(8d+7) + 4^m s^2.$$

Ist $s=0$, so folgt wegen $8|z'$, daß $c' \geq 2$, also $16|z'$.

Nun sei $s > 0$.

Für $\min(c', m) \geq 2$ folgt aus (7) sofort $16|z'$.

Ist $\min(c', m) = 1$, so ist $c' \neq m$ unmöglich, denn nach (7) würde gelten $8 \nmid z'$. Damit ist $c' = m = 1$. Da $s^2 \equiv 1 \pmod{8}$, folgt aus (7) nun

$$z' = 4(8d+7+s^2) \equiv 0 \pmod{32}.$$

In jedem Fall ist $16|z' = \frac{z}{4^r}$, also $4 \mid \frac{z}{4^{r+1}}$. Wäre $z \in E(n^2)$, so würde durch $(r+1)$ -fache Anwendung von Lemma 1 folgen, daß $2|t$ und

$$\frac{z}{4^{r+1}} \in E\left(\left(\frac{n}{2^{r+1}}\right)^2\right) = E\left(\left(\frac{t}{2}\right)^2\right).$$

Da $4 \mid \frac{z}{4^{r+1}}$, würde durch nochmalige Anwendung dieses Lemmas $2 \mid \frac{t}{2}$ folgen, also $4|t$, im Widerspruch zur Voraussetzung. Somit gilt $z \notin E(n^2)$.

Sei nun $r' > 0$.

Damit muß $a'=0$ oder $c'=0$ sein. Aus (6) folgt dann sofort, $a'=c'=0$. Also ist $a=c$ und man hat $r-a=r' > 0$.

Aus (5) folgt wegen $2|x_g$, daß

$$\frac{z}{4^a} = 8d + 7 + 4^{r'} x_g^2 \equiv 7 \pmod{8}.$$

Damit erhalten wir aus

$$\frac{z}{4^a} = y_1^2 + y_2^2 + y_3^2 + y_4^2, \quad y_i \in \mathbb{N}_0, \quad i=1,2,3,4,$$

daß o.B.d.A. gilt

$$y_1^2 \equiv y_2^2 \equiv y_3^2 \equiv 1 \pmod{8} \quad \text{und} \quad y_4^2 \equiv 4 \pmod{8}.$$

Wir betrachten nun

$$z = (2^a y_1)^2 + (2^a y_2)^2 + (2^a y_3)^2 + (2^a y_4)^2.$$

Wegen $a < r$ und $2 \nmid y_i$ für $i=1,2,3$ folgt $2^a y_i \neq 2^r t = n$ für $i=1,2,3$.

Wir nehmen an, es gilt $2^a y_4 = n = 2^r t$.

Es ist $y_4 \equiv 2 \pmod{4}$, so daß wegen $a < r$ gelten muß $r=a+1$ und $r'=1$. Aus (4) folgt dann der Widerspruch

$$7 \equiv \frac{z}{4^a} = 8b + 7 + 4x_u^2 \equiv 3 \pmod{8}.$$

Damit ist $2^a y_i \neq n$ für $i=1,2,3,4$. Somit folgt auch diesmal $z \notin E(n^2)$ ■

Es gilt noch der folgende

Satz 3 (G. Pall). ³⁾

$$E(0^2)$$

$$= \{0, 1, 3, 5, 9, 11, 17, 29, 41, 2^{2k+1}, 3 \cdot 2^{2k+1}, 7 \cdot 2^{2k+1} \mid k \in \mathbb{N}_0\}.$$

Nun zum

Beweis von Satz 1. Nach Lemma 6 gibt es für alle ungeraden t , $t \neq 9$, sowie für $t=10$ und $t=18$ Zahlen $x_u, x_g \in X_t$ mit $2 \nmid x_u \nmid t$, $2 \mid x_g \nmid t$. Zu jedem $n \in \mathbb{N}$, $n \neq 9$ kann eines dieser t

³⁾ Pall [14], S. 11, siehe auch Sierpinski [20], S. 373.

gewählt werden mit $n=2^r t$, $r \in \mathbb{N}_0$.

Wegen 4†t folgt aus Lemma 7 für alle $z \in E(n^2)$, daß
 $z < \max((2^r x_u)^2, (2^r x_g)^2)$. Damit ist $|E(n^2)| < \infty$.

Für ungerade $t > 5$, sowie für $t=10$ und $t=18$ gilt nach
 Lemma 6 darüber hinaus

$$z < \max((2^r x_u)^2, (2^r x_g)^2) < (2^r t)^2 = n^2.$$

Da aber $z > n^2$ sein muß, ist

$$E(n^2) = \emptyset \text{ für alle } n \in \mathbb{N} \text{ mit } n \neq 2^k, 3 \cdot 2^k, 5, 9 \text{ (} k \in \mathbb{N}_0 \text{)}.$$

Nun zeigen wir, daß auch $E(9^2) = \emptyset$. Sei $z \in E(9^2)$. Da,
 wie soeben bewiesen, $E(18^2) = \emptyset$ ist, kann z nach Lemma 1
 nicht gerade sein. Sei also $z \equiv 1, 3, 5$ oder $7 \pmod{8}$. Es
 gilt wegen

$$\begin{aligned} 9^2 + 2^2 &= 7^2 + 6^2 \\ 2 \cdot 9^2 + 2^2 &= 11^2 + 6^2 + 3^2 \\ 3 \cdot 9^2 + 2^2 &= 15^2 + 3^2 + 3^2 + 2^2 \end{aligned}$$

bzw.

$$\begin{aligned} 9^2 + 8^2 &= 12^2 + 1^2 \\ 2 \cdot 9^2 + 8^2 &= 15^2 + 1^2 + 0^2 \\ 3 \cdot 9^2 + 8^2 &= 17^2 + 3^2 + 3^2 + 0^2, \end{aligned}$$

daß $2 \in X_9$ und $8 \in X_9$. Da $z > 9^2$ ist, gilt mit geeignetem
 $x \in \{2, 8\}$, daß $0 < z - x^2 \equiv 7 \pmod{8}$. Aus Satz 2 und
 Lemma 2 folgt $z \notin E(9^2)$, also $E(9^2) = \emptyset$.

Insbesondere folgt auch $|E(n^2)| < \infty$ für alle $n \in \mathbb{N}$. Nach
 Satz 3 ist $|E(0^2)| = \infty$. Damit folgt $\tilde{U} = \{0\}$.

Zum Beweis der Aussage über U muß noch $E(n^2) \neq \emptyset$ für
 $n = 2^k, 3 \cdot 2^k, 5$ ($k \in \mathbb{N}_0$) gezeigt werden.

Zuerst sei $n = 2^k$, $k \in \mathbb{N}_0$.

Es ist $\frac{8}{4} = 2 \in E(1^2) = E((\frac{2}{2})^2)$. Aus Lemma 1 folgt $8 \in E(2^2)$.

Die k-malige Anwendung dieses Lemmas liefert $2^{2k+1} \in E((2^k)^2)$.

Sei nun $n = 3 \cdot 2^k$, $k \in \mathbb{N}_0$. Es ist $14 \in E(3^2)$. Wie zuvor folgt $7 \cdot 2^{2k+1} \in E((3 \cdot 2^k)^2)$.

Schließlich sei $n=5$. Es gilt $79 \in E(3^2)$, denn

$$49 + \underline{25} + 4 + 1 = 36 + \underline{25} + 9 + 9 = \underline{25} + \underline{25} + \underline{25} + 4$$

sind sämtliche wesentlich verschiedene Darstellungen von 79.

Also ist $U = \{0^2, 5^2, (2^k)^2, (3 \cdot 2^k)^2 \mid k \in \mathbb{N}_0\}$ ■

§ 3 "Dünne" Basen,

die nur aus Quadraten bestehen

3.1 Konstante, die im folgenden meist mit C , C_1 , c oder c_i ($i \in \mathbb{N}$) bezeichnet werden, sind, wenn nicht ausdrücklich anders festgelegt, positive reelle Zahlen.

Ziel der Ausführungen in diesem Paragraphen ist der Beweis der beiden folgenden Sätze, wobei sich Satz 5 als Folgerung aus Satz 4 ergibt.

Satz 4. Es sei $\varepsilon > 0$ und $4 \leq h \in \mathbb{N}$.

Dann gibt es für $h=4$ eine Basis $B_{4,\varepsilon}$ der Ordnung 4 für $\{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\}$ und für $h \geq 5$ eine Basis $B_{h,\varepsilon}$ der Ordnung h für $\mathbb{N}$ mit folgenden Eigenschaften:

- (i) $B_{h,\varepsilon}$ besteht nur aus Quadraten ganzer Zahlen.
- (ii) Für ein $C_1 = C_1(h, \varepsilon) > 0$ gilt für alle $n \in \mathbb{N}$

$$B_{h,\varepsilon}(n) \leq C_1 n^{1/h+\varepsilon}.$$
- (iii) Es gibt ein $C_2 = C_2(h, \varepsilon) > 0$, so daß jedes $n \in \mathbb{N}$ höchstens $C_2 n^\varepsilon$ Darstellungen als Summe von h Quadraten aus $B_{h,\varepsilon}$ besitzt.

Satz 5. Für jedes $\varepsilon > 0$ existiert eine Basis B_ε der Ordnung 4 für $\mathbb{N}$, die nur aus Quadraten ganzer Zahlen besteht und eine Konstante $C = C(\varepsilon) > 0$, so daß für alle $n \in \mathbb{N}$ gilt

$$B_\varepsilon(n) \leq C n^{1/4+\varepsilon}.$$

3.2 Zum Beweis von Satz 4 verwenden wir die wahrscheinlichkeits-theoretische Methode, die von Erdős und Rényi [8] in die Zahlentheorie eingeführt wurde. Dazu werden zunächst einige Bezeichnungen und Hilfsmittel zusammengestellt. Eine ausführliche Darstellung dieser Methode findet sich in dem Buch von Halberstam und Roth [9].

Sei X eine nichtleere Menge und $S \subseteq \mathcal{P}(X)$ (⁴) eine σ -Algebra (d.h. S ist bezüglich mengentheoretischer Differenzbildung und bezüglich der Bildung von Vereinigung und Durchschnitt von höchstens abzählbar vielen Mengen aus S abgeschlossen, und es gilt $\emptyset \in S$, $X \in S$).

Eine Funktion μ

$$\mu: S \longrightarrow \mathbb{R}$$

habe die folgenden Eigenschaften:

- 1) $\mu(E) \geq 0$ für alle $E \in S$,
- 2) $\mu(X) = 1$,
- 3) $\mu\left(\bigcup_{j=1}^{\infty} E_j\right) = \sum_{j=1}^{\infty} \mu(E_j)$ für jede Folge $(E_j)_{j \in \mathbb{N}}$ beliebig, paarweise disjunkter $E_j \in S$ (σ -Additivität).

Man bezeichnet μ als Wahrscheinlichkeitsmaß auf S und das Tripel (X, S, μ) als Wahrscheinlichkeitsraum.

Die Teilmengen $E \subseteq X$ nennt man Ereignisse und die Ereignisse $E \in S$ heißen meßbar.

Ist $\mu(E) = 1$ für ein meßbares Ereignis E , so sagt man auch, daß die kennzeichnende Eigenschaft der Elemente von E "mit Wahrscheinlichkeit 1" gilt.

⁴) $\mathcal{P}(X)$ bezeichne die Potenzmenge von X .

Wir bezeichnen $X \setminus E$ durch $\bar{E}$.

Ein endliches oder unendliches Teilsystem S' von S heißt unabhängig, falls

$$\mu\left(\bigcap_{j=1}^n E_j\right) = \prod_{j=1}^n \mu(E_j)$$

für jedes endliche Teilsystem $E_1, E_2, \dots, E_n \in S'$.

Lemma 8. Sei (X, S, μ) ein Wahrscheinlichkeitsraum, dann gilt:

- (i) $\mu(\bar{E}) = 1 - \mu(E)$ für jedes $E \in S$.
- (ii) $\mu(\emptyset) = 0$.
- (iii) Aus $E_1, E_2 \in S$ und $E_1 \subseteq E_2$ folgt $\mu(E_1) \leq \mu(E_2)$.
- (iv) $0 < \mu(E) < 1$ für jedes $E \in S$.
- (v) Für beliebige $E_1, E_2 \in S$ ist

$$\mu(E_1 \cup E_2) = \mu(E_1) + \mu(E_2) - \mu(E_1 \cap E_2).$$
- (vi) Sind $E_1, E_2, \dots, E_n \in S$ und $\mu(E_i) = 1$ für $i=1, 2, \dots, n$, so gilt

$$\mu\left(\bigcap_{i=1}^n E_i\right) = 1.$$
- (vii) Sind $E_1, E_2, \dots, E_n \in S$, so ist

$$\mu\left(\bigcup_{j=1}^n E_j\right) \leq \sum_{j=1}^n \mu(E_j).$$

Gilt für eine Folge $E_1, E_2, \dots \in S$, daß

$$\sum_{j=1}^{\infty} \mu(E_j) < +\infty,$$

so ist

$$\mu\left(\bigcup_{j=1}^{\infty} E_j\right) \leq \sum_{j=1}^{\infty} \mu(E_j).$$

Lemma 9 (Borel - Cantelli).

Sei (X, S, μ) ein Wahrscheinlichkeitsraum, $(E_j)_{j \in \mathbb{I}}$ eine Folge von Ereignissen aus S . Wir setzen

$$\bigcap_{i=1}^{\infty} \bigcup_{j=i}^{\infty} E_j =: E.$$

Gilt

$$\sum_{j=1}^{\infty} \mu(E_j) < +\infty ,$$

so ist

$$\mu(E) = 0 \quad .^5)$$

Für die zahlentheoretische Anwendung der Wahrscheinlichkeitstheorie ist der folgende Satz von grundlegender Bedeutung, dessen Beweis man [9], S. 142 entnehmen kann.

Satz 6. Seien $p(1), p(2), \dots$ reelle Zahlen mit

$$0 \leq p(n) \leq 1 \quad \text{für alle } n \in \mathbb{N}.$$

Dann existiert eine σ -Algebra S in $X := \mathcal{P}(\mathbb{N})$

und ein Wahrscheinlichkeitsmaß P auf S , so daß

(X, S, P) ein Wahrscheinlichkeitsraum mit folgenden Eigenschaften ist:

(i) Für jedes $n \in \mathbb{N}$ ist

$$B^{(n)} := \{U \in X \mid n \in U\} \in S \quad \text{und}$$

$$P(B^{(n)}) = p(n) .$$

(ii) Die Ereignisse $B^{(1)}, B^{(2)}, \dots$ sind unabhängig.⁶⁾

Das Lemma von Borel - Cantelli wird aufgrund dieses Satzes zum Nachweis der Existenz von Mengen natürlicher Zahlen U mit gewissen Eigenschaften, die durch $U \in \bar{E}$ über

⁵⁾ Hier ist nur der einfachere Teil der Aussage des Lemmas von Borel - Cantelli wiedergegeben, da nur dieser benötigt wird.

⁶⁾ Da $X = \mathcal{P}(\mathbb{N})$ ist, kann man statt $U \in X$ auch $U \subseteq \mathbb{N}$ schreiben, was im folgenden immer geschehen soll. Die Elemente der Ereignisse sind daher Mengen natürlicher Zahlen und es gilt $S \subseteq \mathcal{P}(\mathcal{P}(\mathbb{N}))$.

die E_j vorgegeben werden, in folgender Weise verwendet:
Ist die Voraussetzung des Lemmas von Borel - Cantelli erfüllt, so ist $P(E)=0$. Mit Lemma 8 folgt $P(\bar{E})=1$ und somit $\bar{E} \neq \emptyset$.

3.3 Eine Basis der Ordnung $h > 2$ für $\mathbb{N}$ enthält notwendigerweise das Element 0. Zur Formulierung der Vorbereitungen zum Beweis von Satz 4 erweist es sich jedoch als günstiger, nur die positiven Elemente der Basen zu betrachten.

Wir erinnern an folgende Bezeichnung:

Für $A \subseteq \mathbb{N}$ und $h \in \mathbb{N}$ ist

$$h \circ A := \sum_{j=1}^h jA.$$

Es gilt dann offenbar folgendes:

Sei $0 \in B \subseteq \mathbb{N}_0$ und $M \subseteq \mathbb{N}$. Genau dann ist B eine Basis der Ordnung h für M , wenn $M \subseteq h \circ (B \setminus \{0\})$.

Weiter benötigen wir folgende Bezeichnungen:

Seien $j_1, j_2 \in \mathbb{N}$, so heißen die Tupel

$$(u_1, u_2, \dots, u_{j_1}) \in \mathbb{N}^{j_1} \quad \text{und} \quad (v_1, v_2, \dots, v_{j_2}) \in \mathbb{N}^{j_2} \quad 7)$$

elementefremd, falls $\{u_1, u_2, \dots, u_{j_1}\} \cap \{v_1, v_2, \dots, v_{j_2}\} = \emptyset$.

Sei $h \in \mathbb{N}$ und $A = \{a_1, a_2, \dots\} \subseteq \mathbb{N}$ mit $a_1 < a_2 < \dots$.

Für $n \in \mathbb{N}$ sei

$$w_h^A(n) := \sum_{j=1}^h \sum_{\substack{(u_1, u_2, \dots, u_j) \in \mathbb{N}^j \\ u_1 < u_2 < \dots < u_j \\ a_{u_1} + a_{u_2} + \dots + a_{u_j} = n}} 1.$$

7) Für Mengen $A_1, A_2, \dots, A_j$ sei $\prod_{i=1}^j A_i$ das kartesische Produkt und $A^j := \prod_{i=1}^j A_i$, falls $A := A_1 = A_2 = \dots = A_j$.

Mit $\overline{w}_h^A(n)$ bezeichnen wir die maximale Anzahl von paarweise elementefremden Tupeln $(u_1, u_2, \dots, u_j) \in \bigcup_{j=1}^h \mathbb{N}^j$ mit $u_1 < u_2 < \dots < u_j$ und $a_{u_1} + a_{u_2} + \dots + a_{u_j} = n$.

Trivialerweise gilt

$$\overline{w}_h^A(n) \leq w_h^A(n) .$$

Für $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$ sei

$$(8) \quad v_{h, \vec{q}}^A(n) := \sum_{\substack{(u_1, u_2, \dots, u_h) \in \mathbb{N}^h \\ u_1 < u_2 < \dots < u_h \\ q_1 a_{u_1} + q_2 a_{u_2} + \dots + q_h a_{u_h} = n}} 1 .$$

Entsprechend wie oben sei $\overline{v}_{h, \vec{q}}^A(n)$ die maximale Anzahl von paarweise elementefremden Tupeln $(u_1, u_2, \dots, u_h) \in \mathbb{N}^h$ mit $u_1 < u_2 < \dots < u_h$ und $q_1 a_{u_1} + q_2 a_{u_2} + \dots + q_h a_{u_h} = n$.

Es gilt

$$\overline{v}_{h, \vec{q}}^A(n) \leq v_{h, \vec{q}}^A(n) .$$

Für $A' \subseteq A$ ist offensichtlich für alle $n \in \mathbb{N}$

$$w_h^{A'}(n) \leq w_h^A(n) ,$$

$$\overline{w}_h^{A'}(n) \leq \overline{w}_h^A(n) ,$$

$$v_{h, \vec{q}}^{A'}(n) \leq v_{h, \vec{q}}^A(n) ,$$

$$\overline{v}_{h, \vec{q}}^{A'}(n) \leq \overline{v}_{h, \vec{q}}^A(n) .$$

Für $A := \{a_1, a_2, \dots\} \subseteq \mathbb{N}$ mit $a_1 < a_2 < \dots$ und $U \subseteq \mathbb{N}$ sei

$$A^U := \{a_u \mid u \in U\} .$$

Offensichtlich gilt $A^U \subseteq A$, sowie $A^{\mathbb{N}} = A$ und $\mathbb{N}^U = U$.

3.4 Es gilt der folgende

Satz 7 (Erdős, Nathanson).

Sei $M \subseteq \mathbb{N}$, $h \in \mathbb{N}$ und $A \subseteq \mathbb{N}$, $|A| = \infty$ mit

$$M \subseteq h \circ A.$$

Es gelte mit Konstanten $C_3 > 0$, $1 > a > 0$, daß

$$A(n) < C_3 n^a \quad \text{für alle } n \in \mathbb{N}.$$

Außerdem gelte mit weiteren Konstanten $C_4 > 0$

und $ah > b > 0$

$$\overline{w}_h^A(n) > C_4 n^b \quad \text{für alle } n \in M.$$

Dann existiert zu jedem $\varepsilon > 0$ eine Menge $A_\varepsilon \subseteq A$

mit $M \subseteq h \circ A_\varepsilon$ und eine Konstante $C'_5 = C'_5(\varepsilon) > 0$, so

daß gilt

$$A_\varepsilon(n) < C'_5 n^{a - b/h + \varepsilon} \quad \text{für alle } n \in \mathbb{N}. \quad 8)$$

Den Beweis einer allgemeineren Fassung dieses Satzes findet man bei Erdős und Nathanson [7]. Er beruht auf der Konstruktion eines geeigneten Wahrscheinlichkeitsraumes nach Satz 6 und liefert noch mehr als nur die Existenz der Menge A_ε mit den angegebenen Eigenschaften: Solche Mengen existieren mit dem dort gewählten Wahrscheinlichkeitsmaß "mit Wahrscheinlichkeit 1". Für das hier angestrebte Ziel ist diese zusätzliche Aussage wichtig, die wir als Lemma 10 formulieren.

8) Aus $\overline{w}_h^A(n) > C_4 n^b$ für alle $n \in M$ folgt bereits $M \subseteq h \circ A$. Ursprünglich war in [7] nur $\overline{w}_h^A(n) > C'_4 n^b / \log^b n$ vorausgesetzt, weswegen neben $n \in M$ zusätzlich $n > 1$ gefordert werden mußte.

Lemma 10. Es gelten die Voraussetzungen von Satz 7 und
zusätzlich

$$(9) \quad \varepsilon < \frac{b}{h} .$$

Sei

$$(10) \quad s := \frac{b}{ah} - \frac{\varepsilon}{a} .$$

Dann gibt es einen Wahrscheinlichkeitsraum

(X, S, P) mit $X = \mathcal{P}(\mathbb{N})$, für welchen gilt:

(i) $B^{(m)} = \{U \in \mathbb{N} \mid m \in U\} \in S$ und $P(B^{(m)}) = m^{-s}$ für alle $m \in \mathbb{N}$.

(ii) Die Ereignisse $B^{(1)}, B^{(2)}, \dots$ sind unabhängig.

Mit einer Konstanten $C_5 = C_5(\varepsilon) > 0$ gilt dann

$E' := \{U \in \mathbb{N} \mid \text{Für ein } F \subseteq M, |F| < \infty \text{ ist } M \setminus F \subseteq h \circ A^U \text{ und}$

$$A^U(n) \sim C_5 n^{a-b/h+\varepsilon} \text{ für alle } n \in \mathbb{N}\} \in S$$

und

$$P(E') = 1 . \quad 9)$$

Das folgende Lemma findet man bei Halberstam und Roth
[9], S. 147.

Lemma 11. Sei $n \in \mathbb{N}$ und seien $y_1, y_2, \dots, y_n$ nichtnegative
reelle Zahlen. Für jedes $d \in \mathbb{N}$, $d \leq n$ sei

$$f_d := \sum_{\substack{(u_1, u_2, \dots, u_d) \in \mathbb{N}^d \\ u_1 < u_2 < \dots < u_d \leq n}} \prod_{j=1}^d y_{u_j} .$$

Dann gilt

$$f_d \leq \frac{1}{d!} f_1^d .$$

⁹⁾ Eine Menge A_ε nach Satz 7 erhält man damit etwa durch
ein beliebiges $U \in E' (\neq \emptyset)$ mit $A_\varepsilon := A^U \cup F$ (wobei die end-
liche Menge F von U abhängt).

Zur Formulierung des nächsten Lemmas führen wir noch folgende Bezeichnung ein:

Sei $h \in \mathbb{N}$

$$A = \{a_1, a_2, \dots\} \subseteq \mathbb{N}, \quad a_1 < a_2 < \dots \text{ und}$$

$$\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h.$$

Für eine Folge $p(1), p(2), \dots$ von reellen Zahlen gelte (wie in Satz 6)

$$0 < p(m) < 1 \quad \text{für alle } m \in \mathbb{N}.$$

Dann sei für jedes $n \in \mathbb{N}$

$$(11) \quad l_n = l_n(h, A, \vec{q}, p(\cdot)) := \sum_{\substack{(u_1, u_2, \dots, u_h) \in \mathbb{N}^h \\ u_1 < u_2 < \dots < u_h \\ q_1 a_{u_1} + q_2 a_{u_2} + \dots + q_h a_{u_h} = n}} \prod_{i=1}^h p(u_i).$$

Lemma 12. Sei $h \in \mathbb{N}$, $A = \{a_1, a_2, \dots\} \subseteq \mathbb{N}$, $a_1 < a_2 < \dots$ und

$$\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h.$$

Sei $(p(m))_{m \in \mathbb{N}}$ eine Folge von reellen Zahlen

mit $0 < p(m) < 1$ für alle $m \in \mathbb{N}$.

(X, S, P) sei ein Wahrscheinlichkeitsraum mit

$X = \mathcal{P}(\mathbb{N})$ für welchen gilt:

(i) $B^{(m)} = \{U \subseteq \mathbb{N} \mid m \in U\} \in S$ und $P(B^{(m)}) = p(m)$ für alle $m \in \mathbb{N}$.

(ii) Die Ereignisse $B^{(1)}, B^{(2)}, \dots$ sind unabhängig.

Dann ist für alle $n \in \mathbb{N}$ und $d \in \mathbb{N}$

$$E_{n,d} := \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > d\} \in S,$$

und es gilt

$$P(E_{n,d}) < \frac{1}{d!} l_n^d.$$

Beweis. Es sei T_n die Menge aller $(u_1, u_2, \dots, u_h) \in \mathbb{N}^h$ mit $u_1 < u_2 < \dots < u_h$ und $q_1 a_{u_1} + q_2 a_{u_2} + \dots + q_h a_{u_h} = n$.

Sind $\vec{t}_1, \vec{t}_2, \dots, \vec{t}_d \in T_n$, so schreiben wir

$$\vec{t}_j = (u_{1,j}, u_{2,j}, \dots, u_{h,j}) \quad \text{für } j=1, 2, \dots, d.$$

Ist $E_{n,d} = \emptyset$, so gilt die Behauptung trivialerweise.

Sei also $E_{n,d} \neq \emptyset$.

Für $U \subseteq \mathbb{N}$ ist $\bar{V}_{h,\vec{q}}^A U(n)$ nach Definition die maximale Anzahl von paarweise elementefremden Tupeln $(u_1, u_2, \dots, u_h) \in U^h$ mit $u_1 < u_2 < \dots < u_h$ und $q_1 a_{u_1} + q_2 a_{u_2} + \dots + q_h a_{u_h} = n$.

Daher ist

$$E_{n,d} = \{U \subseteq \mathbb{N} \mid \bar{V}_{h,\vec{q}}^A U(n) \geq d\}$$

$$= \{U \subseteq \mathbb{N} \mid \text{Es gibt mindestens } d \text{ paarweise elementefremde}$$

$$\text{Tupel } \vec{t}_1, \vec{t}_2, \dots, \vec{t}_d \in T_n \text{ mit } (u_{1,j}, \dots, u_{h,j}) \in U^h \\ \text{für } j=1, 2, \dots, d\}.$$

$$= \{U \subseteq \mathbb{N} \mid \begin{array}{l} \vec{t}_1, \vec{t}_2, \dots, \vec{t}_d \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ paarw. elem.fr.} \end{array} \quad \bigwedge_{j=1}^d \bigwedge_{i=1}^h u_{i,j} \in U\}$$

$$= \{U \subseteq \mathbb{N} \mid \begin{array}{l} \vec{t}_1, \dots, \vec{t}_d \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ paarw. elem.fr.} \end{array} \quad \bigwedge_{j=1}^d \bigwedge_{i=1}^h U \in B^{(u_{i,j})}\}$$

$$= \begin{array}{l} \vec{t}_1, \dots, \vec{t}_d \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ paarw. elem.fr.} \end{array} \quad \bigcap_{j=1}^d \bigcap_{i=1}^h B^{(u_{i,j})}.$$

Also ist $E_{n,d} \in \mathcal{S}$, da $B^{(m)} \in \mathcal{S}$ für alle $m \in \mathbb{N}$. Nach Lemma 8 (vii) gilt

$$P(E_{n,d}) \leq \sum_{\substack{\vec{t}_1, \dots, \vec{t}_d \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ paarw. elem.fr.}}} P\left(\bigcap_{j=1}^d \bigcap_{i=1}^h B^{(u_{i,j})}\right)$$

$$= \sum_{\substack{\vec{t}_1, \dots, \vec{t}_d \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ paarw. elem.fr.}}} \prod_{j=1}^d \prod_{i=1}^h P(u_{i,j}), \text{ denn die}$$

Ereignisse $B^{(1)}, B^{(2)}, \dots$ mit $P(B^{(m)}) = p(m)$ sind unabhängig, und wegen der paarweisen Elementefremdheit der $\vec{t}_j = (u_{1,j}, \dots, u_{h,j})$ in jeder der Mengen $\{\vec{t}_1, \dots, \vec{t}_d\}$ sind die $u_{i,j}$ paarweise ungleich für $i=1, \dots, h$ und $j=1, \dots, d$.

Die letzte Summe ist gleich

$$\begin{aligned} & \sum_{\substack{(u_{1,1}, u_{1,2}, \dots, u_{1,d}) \in \mathbb{N}^d \\ u_{1,1} < u_{1,2} < \dots < u_{1,d}}} \sum_{\substack{\{\vec{t}_1, \dots, \vec{t}_d\} \in T_n \\ \vec{t}_1, \dots, \vec{t}_d \text{ p. el. fr.}}} \prod_{j=1}^d \prod_{i=1}^h p(u_{i,j}) \\ & < \sum_{\substack{(u_{1,1}, u_{1,2}, \dots, u_{1,d}) \in \mathbb{N}^d \\ u_{1,1} < u_{1,2} < \dots < u_{1,d}}} \sum_{(\vec{t}_1, \dots, \vec{t}_d) \in T_n^d} \prod_{j=1}^d \prod_{i=1}^h p(u_{i,j}) \\ & = \sum_{\substack{(u_{1,1}, \dots, u_{1,d}) \in \mathbb{N}^d \\ u_{1,1} < \dots < u_{1,d}}} \prod_{j=1}^d \sum_{\vec{t}_j = (u_{1,j}, \dots, u_{h,j}) \in T_n} \prod_{i=1}^h p(u_{i,j}) \\ & =: f_d. \end{aligned}$$

Für jedes $u_{1,j} \in \mathbb{N}$ sei

$$y_{u_{1,j}} := \sum_{(u_{1,j}, u_{2,j}, \dots, u_{h,j}) \in T_n} \prod_{i=1}^h p(u_{i,j}),$$

dann folgt aus Lemma 11 wegen

$$d < u_{1,d} \leq a_{u_{1,d}} < n$$

und wegen (11), daß

$$\begin{aligned} f_d & < \frac{1}{d!} f_1^d = \frac{1}{d!} \left(\sum_{u_{1,1} \in \mathbb{N}} \sum_{(u_{1,1}, u_{2,1}, \dots, u_{h,1}) \in T_n} \prod_{i=1}^h p(u_{i,1}) \right)^d \\ & = \frac{1}{d!} \left(\sum_{(u_1, u_2, \dots, u_h) \in T_n} \prod_{i=1}^h p(u_i) \right)^d \\ & = \frac{1}{d!} \left(\sum_{\substack{(u_1, u_2, \dots, u_h) \in \mathbb{N}^h \\ u_1 < u_2 < \dots < u_h \\ q_1 a_{u_1} + \dots + q_h a_{u_h} = n}} \prod_{i=1}^h p(u_i) \right)^d = \frac{1}{d!} 1_n^d \quad \blacksquare \end{aligned}$$

Lemma 13. Es seien c_1 und c_2 reelle Zahlen mit

$$0 < c_1 < c_2.$$

Dann konvergiert die Reihe

$$\sum_{n=1}^{\infty} \frac{c_1^n c_2}{[n^{c_2}]!}.$$

Beweis. Für $n \in \mathbb{N}$ sei $m := [n^{c_2}]$, also $m \geq 1$. Es folgt

$$e^m = 1 + m + \frac{m^2}{2!} + \dots + \frac{m^m}{m!} + \dots > \frac{m^m}{m!}.$$

Also ist

$$\begin{aligned} \frac{n^{c_1 n^{c_2}}}{[n^{c_2}]!} &= \frac{n^{c_1 n^{c_2}}}{m!} < n^{c_1 n^{c_2}} \left(\frac{e}{m}\right)^m = e^{c_1 n^{c_2} \log n + m - m \log m} \\ &< e^{c_1 n^{c_2} \log n + n^{c_2} - (n^{c_2} - 1) \log \left(\frac{n^{c_2}}{2}\right)}, \text{ da} \\ &\qquad\qquad\qquad 2m \geq m+1 > n^{c_2} \\ &< e^{-(c_2 - c_1)n^{c_2} \log n + n^{c_2}(1 + \log 2) + c_2 \log n} \\ &< e^{-c n^{c_2} \log n} \quad \text{für ein } 0 < c < c_2 - c_1 \\ &\qquad\qquad\qquad \text{und alle } n > n_1(c) \\ &< e^{-2 \log n} \quad \text{für alle } n > n_2(c) \\ &= n^{-2}. \end{aligned}$$

Damit ist die Konvergenz der Reihe nachgewiesen ■

Lemma 14. Sei $2 < h \in \mathbb{N}$, $A \in \mathbb{N}$, $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$

und $a, c \in \mathbb{R}$ mit $1 > a > 0$, $c > 0$.

Es gelte für Konstante $C_3 > 0$ und $C_6 > 0$ und für alle $n \in \mathbb{N}$, daß

$$(12) \qquad A(n) < C_3 n^a$$

und

$$(13) \quad v_{h-1, (q_2, q_3, \dots, q_h)}^A(n) \leq c_6 n^c.$$

Für $c_3 \in \mathbb{R}$ mit

$$(14) \quad 0 < c_3 < 1$$

sei

$$(15) \quad s := h^{-1}(1 - c_3).$$

(X, S, P) sei ein Wahrscheinlichkeitsraum mit

$X = \mathcal{G}(\mathbb{N})$ für welchen gilt:

(i) $B^{(m)} = \{U \subseteq \mathbb{N} \mid m \in \mathbb{N}\} \in S$ und $P(B^{(m)}) = m^{-s}$ für alle $m \in \mathbb{N}$.

(ii) Die Ereignisse $B^{(1)}, B^{(2)}, \dots$ sind unabhängig.

Sei $c_2 \in \mathbb{R}$ mit

$$(16) \quad c_2 > c_3 a + c,$$

so ist

$E_{\vec{q}}^u := \{U \subseteq \mathbb{N} \mid \bar{v}_{h, \vec{q}}^A(n) < n^{c_2} \text{ für alle bis auf endlich viele } n \in \mathbb{N}\} \in S$

und es gilt $P(E_{\vec{q}}^u) = 1$.

Beweis. Es sei $n \in \mathbb{N}$. Wegen (14) ist $s > 0$. Nach (11)

ist wegen $p(m) = m^{-s}$ für alle $m \in \mathbb{N}$

$$1_n = 1_n(h, A, \vec{q}, p(\cdot)) = \sum_{\substack{(u_1, u_2, \dots, u_h) \in \mathbb{N}^h \\ u_1 < u_2 < \dots < u_h \\ q_1 a_{u_1} + \dots + q_h a_{u_h} = n}} \prod_{i=1}^h u_i^{-s}$$

$$< \sum_{u_1 \in \mathbb{N}} u_1^{-hs} \sum_{\substack{(u_2, u_3, \dots, u_h) \in \mathbb{N}^{h-1} \\ u_1 < u_2 < u_3 < \dots < u_h \\ q_2 a_{u_2} + q_3 a_{u_3} + \dots + q_h a_{u_h} = n - q_1 a_{u_1}}} 1$$

$$< \sum_{\substack{u \in \mathbb{N} \\ q_1 a_u < n}} u^{c_3-1} v_{h-1, (q_2, q_3, \dots, q_h)}^{(n - q_1 a_u)} \quad \text{wegen} \quad (15) \text{ und } (8)$$

$$< \sum_{\substack{u \in \mathbb{N} \\ q_1 a_u < n}} u^{c_3-1} C_6^{(n - q_1 a_u)^c} \quad \text{wegen } (13).$$

Aus $q_1 a_u < n$ folgt wegen (12)

$$(17) \quad q_1^a u = q_1^a A(a_u) < q_1^a C_3 a_u^a < C_3 n^a.$$

Wir setzen

$$\frac{q_1}{C_3^{1/a}} =: C_7$$

und

$$C_3 \left(\frac{n}{q_1} \right)^a = \left(\frac{n}{C_7} \right)^a =: r$$

Mit (17) erhält man

$$u \leq C_3 \left(\frac{n}{q_1} \right)^a = r$$

und

$$q_1 a_u > q_1 \left(\frac{u}{C_3} \right)^{1/a} = C_7 u^{1/a}.$$

Daher gilt

$$\begin{aligned} 1_n &< C_6 \sum_{1 \leq u \leq r} u^{c_3-1} (n - C_7 u^{1/a})^c \\ &< C_6 \int_1^r u^{c_3-1} (n - C_7 u^{1/a})^c du + (n - C_7)^c \\ &< C_6 r^{c_3} \int_1^r \frac{(n - C_7 u^{1/a})^c}{u} du + n^c, \text{ da } n > C_7 \\ &= C_6 \frac{n^{ac_3}}{C_7^{ac_3}} \int_{1/r}^1 \frac{n^c (1 - y^{1/a})^c}{y} dy + n^c \quad (\text{Substitution:} \\ &\quad y = u \left(\frac{C_7}{n} \right)^a = \frac{u}{r}) \end{aligned}$$

$$< C_8 n^{ac_3+c} \int_{1/r}^1 \frac{dy}{y} + n^c$$

$$= C_8 n^{ac_3+c} \log \left(\frac{n}{C_7} \right)^a + n^c$$

$$< C_9 n^{ac_3+c} \log \left(\frac{n}{C_7} \right)^a$$

$$< n^{c_1} \quad \text{für ein } c_1 \text{ mit } ac_3+c < c_1 < c_2 \text{ und alle } n > n_0.$$

Sei $d := [n^{c_2}]$, dann ist nach Lemma 12

$$\{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2}\} = \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > [n^{c_2}]\} \in \mathcal{S}$$

und

$$P(\{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2}\}) \leq \frac{1}{[n^{c_2}]!} 1_n^{[n^{c_2}]} \leq \frac{1}{[n^{c_2}]!} n^{c_1 n^{c_2}}.$$

Daher konvergiert nach Lemma 13

$$\sum_{n=1}^{\infty} P(\{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2}\}).$$

Das Lemma von Borel - Cantelli (Lemma 9) liefert nun

$$P\left(\bigcap_{m=1}^{\infty} \bigcup_{n=m}^{\infty} \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2}\}\right) = 0$$

Es ist

$$E := \bigcap_{m=1}^{\infty} \bigcup_{n=m}^{\infty} \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2}\} \in \mathcal{S}$$

$$= \bigcap_{m=1}^{\infty} \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2} \text{ für ein } n > m\}$$

$$= \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) > n^{c_2} \text{ für unendlich viele } n \in \mathbb{N}\}.$$

Also

$$\bar{E} = \{U \subseteq \mathbb{N} \mid \bar{v}_{h,\vec{q}}^A(n) \leq n^{c_2} \text{ für höchstens endlich viele } n \in \mathbb{N}\}$$

$$= E_{\vec{q}}'' \in \mathcal{S} \quad \text{und} \quad P(E_{\vec{q}}'') = P(\bar{E}) = 1 \quad \blacksquare$$

Aus den Lemmata 10 und 14 erhalten wir

Satz 8. Seien h_1 und h natürliche Zahlen mit $2 < h < h_1$
und $A \subseteq \mathbb{N}$, $|A| = \infty$, $M \subseteq \mathbb{N}$ mit

$$M \subseteq h \circ A.$$

Es gelte für Konstante $C_3 > 0$ und $1 > a > 0$

$$(18) \quad A(n) < C_3 n^a \quad \text{für alle } n \in \mathbb{N}.$$

Für Konstante $C_4 > 0$ und $b > 0$ mit

$$(19) \quad \frac{a}{2} < b < a$$

sei

$$(20) \quad \overline{w}_h^A(n) > C_4 n^b \quad \text{für alle } n \in M. \quad 10)$$

Für Konstante $C_6 > 0$ und $c > 0$ gelte für jedes
 $(q_2, q_3, \dots, q_h) \in \mathbb{N}^{h-1}$ mit $q_2 + q_3 + \dots + q_h < h_1$ und
jedes $n \in \mathbb{N}$

$$(21) \quad v_{h-1}^A(q_2, q_3, \dots, q_h) < C_6 n^c.$$

Es sei noch

$$(22) \quad c_2 > 2(a-b) + c.$$

Dann gibt es eine Menge $A' \subseteq A$ mit

$$M \subseteq h \circ A'$$

und Konstante $C_{10} > 0$, $C_{11} > 0$, so daß gilt

$$(23) \quad A'(n) < C_{10} n^{a - \frac{2b-a}{h}} \quad \text{für alle } n \in \mathbb{N}$$

und

$$(24) \quad \overline{v}_{h, \vec{q}}^{A'}(n) < C_{11} n^{c_2} \quad \text{für alle } n \in \mathbb{N}$$

und für alle $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$ mit

$$q_1 + q_2 + \dots + q_h \leq h_1.$$

¹⁰⁾ (20) schließt natürlich $M \subseteq h \circ A$ ein.

Beweis. Zur Anwendung von Lemma 10 und 14 werden für die dort auftretenden Mengen A und M die ebenso bezeichneten Mengen in der Voraussetzung des hier zu beweisenden Satzes gewählt. Entsprechendes gilt für die Konstanten $h, a, b, c, C_3, C_4, C_6$, sowie für $\bar{q}$. (Man beachte, daß c und C_6 universelle Konstante für alle in der Voraussetzung betrachteten $\bar{q}$ sind.)

In Lemma 10 wählen wir

$$\varepsilon := \frac{a-b}{h} .$$

Wegen (19) folgt (9) und

$$ha > a > b > 0 .$$

Mit (18) und (20) sind die übrigen Voraussetzungen von Lemma 10 (siehe auch Satz 7) erfüllt.

Wir betrachten den Wahrscheinlichkeitsraum (X, S, P) nach Lemma 10. Es folgt für eine Konstante $C_5 > 0$

$$(25) \quad E' = \{U \in \mathbb{N} \mid \text{Für ein } F \subseteq M, |F| < \infty \text{ ist } M \setminus F \subseteq h \circ A^U \text{ und} \\ A^U(n) \sim C_5 n^{a - \frac{b}{h} + \frac{a-b}{h}} \mid \in S$$

und

$$(26) \quad P(E') = 1 .$$

In Lemma 14 wählen wir

$$c_3 := 2(1 - \frac{b}{a}) .$$

Wegen (19) gilt $0 < c_3 = 2 - \frac{2b}{a} < 1$ und damit (14).

Mit dieser Wahl von c_3 hat s in Lemma 14 den gleichen Wert wie in Lemma 10 (siehe (15) und (10)):

$$s = h^{-1}(1 - c_3) = h^{-1}(1 - 2(1 - \frac{b}{a})) = \frac{b}{ah} - \frac{a-b}{ah} = \frac{b}{ah} - \frac{\varepsilon}{a} .$$

Der Wahrscheinlichkeitsraum (X, S, P) aus Lemma 10 erfüllt daher die Voraussetzungen (i) und (ii) in Lemma 14.

Mit (22)

$$c_2 > 2(a-b) + c = c_3 a + c$$

gilt (16) und mit (18) und (21) gelten auch (12) und (13).

Damit folgt aus Lemma 14 für jedes $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$

mit $q_1 + q_2 + \dots + q_h < h_1$, daß

$$E''_{\vec{q}} = \{U \in \mathbb{N} \mid \bar{V}_{h, \vec{q}}^{A^U}(n) < n^{c_2} \text{ für alle bis auf endlich viele } n \in \mathbb{N}\} \in S$$

$$\text{und} \quad P(E''_{\vec{q}}) = 1.$$

Es gibt nur endlich viele $\vec{q} \in \mathbb{N}^h$ mit $q_1 + q_2 + \dots + q_h < h_1$.

Wegen (26) folgt aus Lemma 8 (vi)

$$P(E' \cap \bigcap_{\substack{\vec{q} \in \mathbb{N}^h \\ q_1 + \dots + q_h \leq h_1}} E''_{\vec{q}}) = 1.$$

Es existiert also eine Menge $U \in E' \cap \bigcap_{\substack{\vec{q} \in \mathbb{N}^h \\ q_1 + \dots + q_h \leq h_1}} E''_{\vec{q}} \neq \emptyset$

und wir betrachten A^U .

Nach (25) gibt es zu $U \in E'$ eine Menge $F \subseteq M$, $|F| < \infty$ mit

$M \setminus F \subseteq h \circ A^U$. Da $M \subseteq h \circ A$ und $A^U \subseteq A$ gilt, sind zur Darstellung der endlich vielen Elemente von F nur endlich viele Elemente aus A erforderlich, die wir zu einer endlichen Menge $\tilde{A}$ zusammenfassen. Damit gilt für

$$A' := A^U \cup \tilde{A} \subseteq A,$$

daß $M \subseteq h \circ A'$. Nach (25) gilt $A'(n) \sim A^U(n) \sim C_5 n^{a - \frac{b}{h} + \frac{a-b}{h}}$.

Für ein geeignetes $C_{10} > C_5 > 0$ ist nun

$$A'(n) < C_{10} n^{a - \frac{b}{h} + \frac{a-b}{h}} = C_{10} n^{a - \frac{2b-a}{h}} \quad \text{für alle } n \in \mathbb{N},$$

womit (23) gezeigt ist.

Sei $\vec{q} \in \mathbb{N}^h$ mit $q_1 + q_2 + \dots + q_h < h_1$. Da $U \in E''_{\vec{q}}$ ist, wird

$\bar{v}_{h,\vec{q}}^{A^U}(n) < n^{c_2}$ von höchstens endlich vielen n nicht erfüllt; es existiert also eine Konstante $C'_{12}(\vec{q}) > 0$ mit $\bar{v}_{h,\vec{q}}^{A^U}(n) \leq C'_{12}(\vec{q}) n^{c_2}$ für alle $n \in \mathbb{N}$. Sei

$$C_{12} := \max\{C'_{12}(\vec{q}) \mid \vec{q} \in \mathbb{N}^h, q_1 + q_2 + \dots + q_h \leq h_1\},$$

so gilt

$$(27) \quad \bar{v}_{h,\vec{q}}^{A^U}(n) \leq C_{12} n^{c_2} \quad \text{für alle } n \in \mathbb{N} \\ \text{und alle } \vec{q} \in \mathbb{N}^h \text{ mit } q_1 + q_2 + \dots + q_h \leq h_1.$$

Zu A' bzw. zu $\tilde{A}$ gibt es eineindeutig zugeordnete Indexmengen U' bzw. $\tilde{U}$ mit $A' = A^{U'}$ bzw. $\tilde{A} = A^{\tilde{U}}$, wobei $|\tilde{U}| = |\tilde{A}| < \infty$. Wegen $A^{U'} = A' = A^U \cup \tilde{A} = A^U \cup A^{\tilde{U}}$ gilt $U' = U \cup \tilde{U}$.

Sei $n \in \mathbb{N}$ und $\vec{q} \in \mathbb{N}^h$ mit $q_1 + q_2 + \dots + q_h \leq h_1$. Unter den $\bar{v}_{h,\vec{q}}^{A^{U'}}(n)$ Tupeln $(u_1, u_2, \dots, u_h) \in U'^h$ können wegen deren paarweiser Elementefremdheit höchstens $|\tilde{U}|$ dieser Tupel ein Element aus $\tilde{U}$ enthalten. Die übrigen enthalten nur Elemente aus U . Von letzteren kann es nicht mehr als $\bar{v}_{h,\vec{q}}^{A^U}(n)$ geben. Es folgt

$$\bar{v}_{h,\vec{q}}^{A^{U'}}(n) \leq \bar{v}_{h,\vec{q}}^{A^U}(n) + |\tilde{U}|.$$

Die endliche Menge $\tilde{U}$ hängt von F , also nur von U ab.

Wegen (27) ist daher mit einem geeigneten $C_{11} > C_{12}$

$$\bar{v}_{h,\vec{q}}^{A'}(n) = \bar{v}_{h,\vec{q}}^{A^{U'}}(n) \leq C_{12} n^{c_2} + |\tilde{U}| \leq C_{11} n^{c_2} \quad \text{für}$$

alle $n \in \mathbb{N}$ und alle $\vec{q} \in \mathbb{N}^h$, $q_1 + q_2 + \dots + q_h \leq h_1$. Damit ist auch (24) gezeigt ■

3.5 Als nächstes beweisen wir eine Verallgemeinerung eines Lemmas von Erdős und Nathanson [7], S. 6-7.

Lemma 15. Sei $A \subseteq \mathbb{N}$ und $2 \leq h \in \mathbb{N}$.

Für eine monoton wachsende Folge $(t_1(n))_{n \in \mathbb{N}}$ nicht-negativer reeller Zahlen sei

$$w_{h-1}^A(n) < t_1(n) \quad \text{für alle } n \in \mathbb{N}.$$

Dann gilt

$$w_h^A(n) < h \bar{w}_h^A(n) t_1(n) \quad \text{für alle } n \in \mathbb{N}.$$

Beweis. Für jedes $n \in \mathbb{N}$ sei T_n die Menge der $w_h^A(n)$ Tupel $(b_1, b_2, \dots, b_j) \in A^j$ mit $b_1 \leq b_2 \leq \dots \leq b_j$ und $b_1 + b_2 + \dots + b_j = n$, wobei j die Werte $1, 2, \dots, h$ durchläuft. T'_n sei eine Menge von $\bar{w}_h^A(n)$ ebensolchen Tupeln, die paarweise elementefremd sind.

Offensichtlich ist $T_n = \emptyset$ genau dann, wenn $T'_n = \emptyset$. In diesem Fall gilt $w_h^A(n) = 0 = \bar{w}_h^A(n)$, woraus die Behauptung folgt.

Sei also $T_n \neq \emptyset \neq T'_n$ und $(b'_1, b'_2, \dots, b'_j) \in T'_n$. Die Anzahl der Tupel aus T_n , welche ein festes b'_i aus $(b'_1, b'_2, \dots, b'_j)$ enthalten, ist gleich $w_{h-1}^A(n - b'_i)$. Die Anzahl der Tupel aus T_n , die wenigstens eine der Zahlen $b'_1, b'_2, \dots, b'_j$ enthalten, ist größer oder gleich

$$\sum_{i=1}^j w_{h-1}^A(n - b'_i) < \sum_{i=1}^j t_1(n - b'_i) < j t_1(n) < h t_1(n),$$

da (t_1) monoton wächst.

Es gibt $\bar{w}_h^A(n)$ elementefremde Tupel in T'_n . Also folgt

$$w_h^A(n) < \bar{w}_h^A(n) \cdot h t_1(n) \quad \blacksquare$$

Lemma 16. Sei $A \subseteq \mathbb{N}$, $2 \leq h \in \mathbb{N}$ und $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$.

Für eine monoton wachsende Folge $(t_2(n))_{n \in \mathbb{N}}$

nicht-negativer reeller Zahlen sei

$$v_{h-1}^A(q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_h)^{(n)} \leq t_2(n)$$

für jedes $n \in \mathbb{N}$ und jedes $i \in \{1, 2, \dots, h\}$.

Dann gilt für alle $n \in \mathbb{N}$

$$v_{h, \vec{q}}^A(n) \leq h^2 \bar{v}_{h, \vec{q}}^A(n) t_2(n) \quad .$$

Beweis. Für jedes $n \in \mathbb{N}$ sei, ähnlich wie im Beweis des

vorangehenden Lemmas, T_n die Menge der $v_{h, \vec{q}}^A(n)$ Tu-

pel $(b_1, b_2, \dots, b_h) \in A^h$ mit $b_1 < b_2 < \dots < b_h$ und

$q_1 b_1 + q_2 b_2 + \dots + q_h b_h = n$. Es sei T_n^i eine Menge von $\bar{v}_{h, \vec{q}}^A(n)$

ebensolchen Tupeln, die paarweise elementefremd sind.

Wieder können wir o.B.d.A. voraussetzen, daß $T_n \neq \emptyset \neq T_n^i$.

Sei $(b_1^i, b_2^i, \dots, b_h^i) \in T_n^i$. Wir betrachten die Tupel aus T_n ,

welche ein festes b_i^i aus $(b_1^i, b_2^i, \dots, b_h^i)$ enthalten. Sie

haben die Form

$$(b_1, \dots, b_{j-1}, b_i^i, b_{j+1}, \dots, b_h) \quad .$$

Es folgt

$$n - q_j b_i^i = q_1 b_1 + \dots + q_{j-1} b_{j-1} + q_{j+1} b_{j+1} + \dots + q_h b_h \quad .$$

Die Anzahl der Tupel $(b_1, \dots, b_{j-1}, b_i^i, b_{j+1}, \dots, b_h) \in T_n$

ist daher größer oder gleich

$$\sum_{j=1}^h v_{h-1}^A(q_1, \dots, q_{j-1}, q_{j+1}, \dots, q_h)^{(n - q_j b_i^i)} \leq h t_2(n) \quad .$$

Die Anzahl der Tupel aus T_n , die wenigstens eine der

Zahlen $b_1^i, b_2^i, \dots, b_h^i$ enthalten, ist somit größer oder

gleich

$$h^2 t_2(n) \quad .$$

Es gibt $\bar{v}_{h,\vec{q}}^A(n)$ elementefremde Tupel $(b_1^i, b_2^i, \dots, b_h^i)$ in T_n^i . Daher folgt

$$v_{h,\vec{q}}^A(n) \leq \bar{v}_{h,\vec{q}}^A(n) \cdot h^2 t_2(n) \blacksquare$$

Lemma 17. Sei $A \in \mathbb{N}$ und $2 \leq h \in \mathbb{N}$.

Es sei $(t_3(n))_{n \in \mathbb{N}}$ eine monoton wachsende Folge nicht-negativer reeller Zahlen, so daß für alle $k \in \mathbb{N}$, $k \leq h$ und alle $\vec{q} = (q_1, q_2, \dots, q_k) \in \mathbb{N}^k$ mit $q_1 + q_2 + \dots + q_k \leq h$ gelte

$$(28) \quad \bar{v}_{k,\vec{q}}^A(n) \leq t_3(n) \quad \text{für alle } n \in \mathbb{N}.$$

Dann ist

$$\bar{w}_h^A(n) \leq (2^h - 1) t_3(n) \quad \text{für alle } n \in \mathbb{N}.$$

Beweis. Sei $n \in \mathbb{N}$. Wir wählen eine beliebige maximale Menge $T^{(n)}$ von $\bar{w}_h^A(n)$ paarw. elementefremden Tupeln $(b_1, \dots, b_j) \in A^j$ mit $b_1 \leq b_2 \leq \dots \leq b_j$ und $b_1 + b_2 + \dots + b_j = n$, wobei $j = 1, 2, \dots, h$. Für $j \in \{1, 2, \dots, h\}$, $k \in \{1, 2, \dots, j\}$ und $\vec{q} = (q_1, q_2, \dots, q_k) \in \mathbb{N}^k$ mit $q_1 + q_2 + \dots + q_k = j$ sei $T_{j,k,\vec{q}}^{(n)}$ die Menge aller $(b_1, \dots, b_j) \in T^{(n)}$ mit

$$b_1 = b_2 = \dots = b_{q_1} < b_{q_1+1} = \dots = b_{q_1+q_2} < b_{q_1+q_2+1} = \dots \\ \dots < b_{q_1+\dots+q_k+1} = \dots = b_{q_1+\dots+q_k} = b_j.$$

Damit ist

$$(29) \quad T^{(n)} = \bigcup_{j=1}^h \bigcup_{k=1}^j \bigcup_{\substack{\vec{q} \in \mathbb{N}^k \\ q_1+\dots+q_k=j}} T_{j,k,\vec{q}}^{(n)}.$$

Sei

$$b^{(1)} := b_1 = b_{q_1}, \quad b^{(2)} := b_{q_1+q_2}, \quad \dots, \quad b^{(k)} := b_{q_1+\dots+q_k},$$

so folgt

$$b^{(1)} < b^{(2)} < \dots < b^{(k)}$$

und

$$n = b_1 + b_2 + \dots + b_j = q_1 b^{(1)} + q_2 b^{(2)} + \dots + q_k b^{(k)}.$$

Daher kann die Anzahl der Tupel aus $T_{j,k,\vec{q}}^{(n)}$ nach oben durch $\bar{v}_{k,\vec{q}}^A(n)$ abgeschätzt werden. Aus (29) und (28) folgt

$$\begin{aligned} \bar{w}_h^A(n) &< \sum_{j=1}^h \sum_{k=1}^j \sum_{\substack{\vec{q} \in \mathbb{N}^k \\ q_1 + \dots + q_k = j}} \bar{v}_{k,\vec{q}}^A(n) \\ &< t_3(n) \sum_{j=1}^h \sum_{k=1}^j \sum_{\substack{\vec{q} \in \mathbb{N}^k \\ q_1 + \dots + q_k = j}} 1 \\ &= t_3(n) \sum_{j=1}^h \sum_{k=1}^j \binom{j-1}{k-1} \\ &= t_3(n) \sum_{j=1}^h 2^{j-1} \\ &= t_3(n) (2^h - 1), \end{aligned}$$

denn jeder Lösung von $q_1 + \dots + q_k = j$ mit $q_l \in \mathbb{N}$ für $l=1, \dots, k$ entspricht genau eine Zerlegung des Intervalls $[0, j]$ durch $k-1$ Teilungspunkte, die ohne Wiederholung und ohne Berücksichtigung der Anordnung aus den Werten $1, 2, \dots, j-1$ entnommen werden. Da die Zuordnung umkehrbar eindeutig ist, erhält man $\binom{j-1}{k-1}$ Lösungen von $q_1 + \dots + q_k = j$ mit $q_l \in \mathbb{N}$ für $l=1, \dots, k$ ■

Lemma 18. Es seien h und h_1 natürliche Zahlen mit

$3 < h < h_1$. Für Mengen $M \subseteq \mathbb{N}$ und $A \subseteq \mathbb{N}$ mit $|A| = \infty$

sei $M \subseteq h \circ A$.

Für Konstante $C_i > 0$ ($i=13,3,14,6,15$) und $c > 0$ mit

$$(30) \quad c < \frac{1}{5(h-1)}$$

gelte

$$(31) \quad w_h^A(n) > C_{13} n^{\frac{1}{h-1}-c} \quad \text{für alle } n \in M, \quad 11)$$

$$(32) \quad A(n) < C_3 n^{\frac{1}{h-1}+c} \quad \text{für alle } n \in \mathbb{N},$$

$$(33) \quad w_{h-1}^A(n) < C_{14} n^c \quad \text{für alle } n \in \mathbb{N},$$

$$(34) \quad v_{h-1, \vec{q}}^A(n) < C_6 n^c \quad \text{für alle } n \in \mathbb{N} \text{ und}$$

alle $\vec{q}' = (q_2, q_3, \dots, q_h) \in \mathbb{N}^{h-1}$ mit $q_2 + q_3 + \dots + q_h < h_1$,
sowie

$$(35) \quad \bar{v}_{k, \vec{q}}^A(n) < C_{15} n^c \quad \text{für alle } n \in \mathbb{N}, \text{ alle}$$

$k \in \{1, 2, \dots, h-1\}$ und alle $\vec{q} = (q_1, q_2, \dots, q_k) \in \mathbb{N}^k$
mit $q_1 + q_2 + \dots + q_k < h_1$.

Dann existieren eine Menge $A' \subseteq A$ mit $M \subseteq h \circ A'$

und Konstante $C'_i > 0$ ($i=3,14,6,15$), so daß

$$(32') \quad A'(n) < C'_3 n^{\frac{1}{h}+3c} \quad \text{für alle } n \in \mathbb{N},$$

$$(33') \quad w_h^{A'}(n) < C'_{14} n^{9c} \quad \text{für alle } n \in \mathbb{N},$$

$$(34') \quad v_{h, \vec{q}}^{A'}(n) < C'_6 n^{9c} \quad \text{für alle } n \in \mathbb{N} \text{ und}$$

alle $\vec{q} = (q_1, q_2, \dots, q_h) \in \mathbb{N}^h$ mit $q_1 + q_2 + \dots + q_h < h_1$,
sowie

$$(35') \quad \bar{v}_{k, \vec{q}}^{A'}(n) < C'_{15} n^{9c} \quad \text{für alle } n \in \mathbb{N}, \text{ alle}$$

$k \in \{1, 2, \dots, h\}$ und alle $\vec{q} = (q_1, q_2, \dots, q_k) \in \mathbb{N}^k$ mit
 $q_1 + q_2 + \dots + q_k < h_1$.

11) (31) schließt natürlich $M \subseteq h \circ A$ ein.

Beweis. Zur Anwendung von Satz 8 behalten A, M, h, h_1 , c, C_3 und C_6 ihre Bedeutung bei. Die dort auftretenden Größen a und b werden wie folgt gewählt:

$$(36) \quad a := \frac{1}{h-1} + c$$

$$(37) \quad b := \frac{1}{h-1} - 2c$$

Wegen (33) und (31) folgt aus Lemma 15 mit

$$(38) \quad t_1(n) := C_{14} n^c > w_{h-1}^A(n) \quad \text{für alle } n \in \mathbb{N},$$

daß für alle $n \in M$ gilt

$$\begin{aligned} \bar{w}_h^A(n) &> \frac{w_h^A(n)}{h t_1(n)} \\ &> \frac{C_{13} n^{\frac{1}{h-1}-c}}{h C_{14} n^c} \\ &=: C_4 n^{\frac{1}{h-1}-2c}, \text{ also mit (37)} \\ &= C_4 n^b. \end{aligned}$$

Somit ist (20) erfüllt.

Wegen (30) gilt

$$-\frac{1}{h-1} + 5c < 0.$$

Damit erhalten wir aus (36) und (37) die Voraussetzung (19) von Satz 8 folgendermaßen

$$b < a = \frac{1}{h-1} + c = \left(\frac{2}{h-1} - \frac{1}{h-1} \right) + (5c - 4c) < \frac{2}{h-1} - 4c = 2b.$$

Wegen (36), (30) und $h \geq 3$ ist

$$0 < a = \frac{1}{h-1} + c < \frac{6}{5(h-1)} < 1.$$

Nach Voraussetzung ((32) und (34)) gelten (18) und (21).

Wir setzen

$$c_2 := 8c.$$

Dann ist (22) wegen (36) und (37) erfüllt, denn

$$2(a-b) + c = 2\left(\frac{1}{h-1} + c - \frac{1}{h-1} + 2c\right) + c = 7c < 8c = c_2.$$

Für den Exponenten in (23) gilt

$$\begin{aligned} a - \frac{2b-a}{h} &= \frac{1}{h-1} + c - \frac{\frac{2}{h-1} - 4c - \frac{1}{h-1} - c}{h} \\ &= \frac{1}{h-1} - \frac{1}{h(h-1)} + c + \frac{5c}{h} \\ &= \frac{1}{h} + c + \frac{5c}{h} \\ &< \frac{1}{h} + 3c, \quad \text{da } h > 3. \end{aligned}$$

Es gibt also nach Satz 8 eine Menge $A' \subseteq A$ mit $M \subseteq h \circ A'$, so daß gilt

$$(39) \quad A'(n) < C_{10} n^{\frac{1}{h}+3c} =: C'_3 n^{\frac{1}{h}+3c} \quad \text{und}$$

$$(40) \quad \bar{V}_{h,\vec{q}}^{A'}(n) < C_{11} n^{c_2} = C_{11} n^{8c}$$

für alle $n \in \mathbb{N}$ und alle $\vec{q} \in H_1^{(h)}$, wobei

$$(41) \quad H_1^{(j)} := \{(q_1, q_2, \dots, q_j) \in \mathbb{N}^j \mid q_1 + q_2 + \dots + q_j < h_1\}$$

für $j \in \{1, 2, \dots, h\}$.

Wegen $A' \subseteq A$ folgt aus (35), daß

$$\begin{aligned} \bar{V}_{k,\vec{q}}^{A'}(n) &< \bar{V}_{k,\vec{q}}^A(n) \\ &< C_{15} n^c \\ &< C_{15} n^{8c} \end{aligned}$$

für alle $k \in \{1, 2, \dots, h-1\}$, alle $\vec{q} \in H_1^{(k)}$ und alle $n \in \mathbb{N}$.

Damit erhalten wir aus (40), indem wir $C'_{15} := \max(C'_{11}, C'_{15})$ wählen:

$$(42) \quad \bar{V}_{k,\vec{q}}^{A'}(n) < C'_{15} n^{8c}$$

für alle $k \in \{1, 2, \dots, h-1, h\}$, alle $\vec{q} \in H_1^{(k)}$ und alle $n \in \mathbb{N}$.

Die Voraussetzung von Lemma 16 ist mit (34) für A' erfüllt:

$$v_{h-1, \vec{q}}^{A'}(n) < v_{h-1, \vec{q}}^A(n) < C_6 n^c =: t_2(n)$$

für alle $\vec{q} \in H_1^{(h-1)}$ und alle $n \in \mathbb{N}$.

Aus Lemma 16 folgt wegen (40) nun

$$(43) \quad v_{h, \vec{q}}^{A'}(n) < h^2 \bar{v}_{h, \vec{q}}^{A'}(n) \cdot t_2(n) < h^2 C_{11} n^{8c} \cdot C_6 n^c =: C'_6 n^{9c}$$

für alle $\vec{q} \in H_1^{(h)}$ und alle $n \in \mathbb{N}$.

Wegen (42) ist

$$\bar{v}_{k, \vec{q}}^{A'}(n) < C'_{15} n^{8c} =: t_3(n)$$

für alle $k \in 1, 2, \dots, h$, alle $\vec{q} \in H_1^{(k)}$ und alle $n \in \mathbb{N}$.

Daher folgt für A' aus Lemma 17, daß

$$(44) \quad \bar{w}_h^{A'}(n) < (2^h - 1) C'_{15} n^{8c} \quad \text{für alle } n \in \mathbb{N}.$$

Wegen $A \supseteq A'$ erhalten wir aus (38) für alle $n \in \mathbb{N}$

$$t_1(n) = C_{14} n^c > w_{h-1}^A(n) > w_{h-1}^{A'}(n).$$

Wir wenden nochmals Lemma 15 an, diesmal jedoch mit A' , an-
statt A und erhalten unter Beachtung von (44) dann für
alle $n \in \mathbb{N}$

$$\begin{aligned} w_h^{A'}(n) &< h \bar{w}_h^{A'}(n) \cdot t_1(n) \\ &< h(2^h - 1) C'_{15} n^{8c} \cdot C_{14} n^c \\ &=: C'_{14} n^{9n}. \end{aligned}$$

Damit folgt (33'). Die Ungleichungen (32'), (34') bzw.
(35') ergeben sich aus (39), (43) bzw. (42) ■

Lemma 19. Sei $2 < h \in \mathbb{N}$, $A \in \mathbb{N}$ und $n \in \mathbb{N}$.

- a) Sei $m \in \mathbb{N}$. Für m paarweise verschiedene $b_j \in A$
($j=1, 2, \dots, m$) sei $n - b_j$ als Summe von höchstens
 $h-1$ Summanden aus A darstellbar.

Dann ist

$$\frac{m}{h} \leq w_h^A(n) .$$

b) Ist $N = (h-1) \cdot A$, so gilt

$$\frac{A(n)}{h} \leq w_h^A(n) .$$

Beweis. a) Sei $B_1 := \{b_1, b_2, \dots, b_m\} \subseteq A$. Es gilt $|B_1| = m$. Für $k \in \mathbb{N}$ sei $B_k \subseteq A$ bereits konstruiert und falls $B_k \neq \emptyset$ ist, so gelte $|B_k| \geq m - (k-1)h$.

Ist $B_k \neq \emptyset$, so gibt es ein $b^{(k)} \in B_k$ mit

$$(45) \quad n - b^{(k)} = \sum_{i=1}^{h-1} a_{i,k} , \text{ wobei } a_{i,k} \in A \cup \{0\}$$

nach Voraussetzung. Dann sei

$$(46) \quad B_{k+1} := B_k \setminus \{b^{(k)}, a_{1,k}, a_{2,k}, \dots, a_{h-1,k}\} \subseteq B_k .$$

Es folgt $|B_{k+1}| \geq m - kh$.

Andernfalls sei $B_{k+1} := B_k = \emptyset$.

Für $k = 1, 2, \dots, \langle \frac{m}{h} \rangle$ ist

$$|B_k| \geq m - (k-1)h \geq m - (\langle \frac{m}{h} \rangle - 1)h > 0 ,$$

also $B_k \neq \emptyset$. Es gibt daher $\langle \frac{m}{h} \rangle$ Zahlen $b^{(k)} \in B_k \neq \emptyset$, so daß (45) und (46) gelten. Es folgt die Existenz von $\langle \frac{m}{h} \rangle$ Darstellungen

$$n = b^{(k)} + \sum_{i=1}^{h-1} a_{i,k} , \quad k=1, 2, \dots, \langle \frac{m}{h} \rangle ,$$

welche jeweils h Summanden aus $A \cup \{0\}$, also höchstens h Summanden aus A besitzen.

Es handelt sich dabei um paarweise wesentlich verschiedene Darstellungen. Denn betrachtet man für $1 \leq k < l \leq \langle \frac{m}{h} \rangle$ die beiden Darstellungen

$$n = b^{(k)} + \sum_{i=1}^{h-1} a_{i,k}$$

und

$$n = b^{(1)} + \sum_{i=1}^{h-1} a_{i,1} ,$$

so ist nach Konstruktion

$$b^{(1)} \in B_1 \subseteq B_k \setminus \{b^{(k)}, a_{1,k}, a_{2,k}, \dots, a_{h-1,k}\} ,$$

$$\text{also } b^{(1)} \neq b^{(k)}$$

$$\text{und } b^{(1)} \neq a_{i,k} \text{ für } i=1,2,\dots,h-1.$$

- Es folgt $\frac{m}{h} < \langle \frac{m}{h} \rangle < w_h^{A(n)}$ und damit die Behauptung.

b) Nach Voraussetzung läßt sich jedes $n \in \mathbb{N}$ als Summe von höchstens $h-1$ Summanden aus A darstellen. Sei

$A = \{a_1, a_2, \dots\}$, wobei $a_1 < a_2 < \dots$, so sind insbesondere die Zahlen $n - a_j$ für jedes $a_j \leq n$, also für jedes $j \in \{1, 2, \dots, A(n)\}$ als Summe von höchstens $h-1$ Summanden aus A darstellbar. Die Behauptung folgt nun mit $m = A(n)$ aus Teil a) ■

Lemma 20. Sei $2 < h \in \mathbb{N}$, $B_i \subseteq \mathbb{N}_0$ für $i=1,2,\dots,h$ und $M \in \mathbb{N}_0$.

Gilt.

$$M \subseteq B_1 + B_2 + \dots + B_h ,$$

dann ist für jedes $n \in \mathbb{N}$

$$M(n) < \prod_{i=1}^h (B_i(n) + 1) .$$

Insbesondere gibt es für eine Basis $B \subseteq \mathbb{N}_0$ der Ordnung h eine Konstante $C_{16} > 0$, so daß für alle $n \in \mathbb{N}$ gilt

$$B(n) > C_{16} n^{1/h} .$$

Beweis. Es gibt genau $\prod_{i=1}^h (B_i(n)+1)$ Tupel

$$(b_1, b_2, \dots, b_h) \in \prod_{i=1}^h ((B_i \cap [0, n]) \cup \{0\}).$$

Wegen

$$M \cap [0, n] \subseteq \sum_{i=1}^h ((B_i \cap [0, n]) \cup \{0\})$$

folgt

$$M(n) < \prod_{i=1}^h (B_i(n)+1)$$

wie behauptet.

Ist $B \subseteq \mathbb{N}_0$ Basis der Ordnung h , so folgt aus dem soeben Gezeigten

$$B(n) > n^{1/h} - 1 \quad \text{für alle } n \in \mathbb{N}.$$

Wegen $1 \in B$ ist $B(n) > 0$ für alle $n \in \mathbb{N}$. Daraus ergibt sich die erwähnte Folgerung ■

3.6 Im folgenden bezeichne Q wieder die Menge der Quadrate der natürlichen Zahlen.

Lemma 21. Sei $d \in \mathbb{Z}$, $k \in \mathbb{N}$ und $\tau(k) := \sum_{t|k} 1$.

Die Lösungsanzahl der quadratischen Kongruenz

$$z^2 \equiv d \pmod{4k}, \quad 0 \leq z < 2k$$

ist kleiner oder gleich

$$2\sqrt{|d|} \cdot \tau(k).$$

Beweis. Die gesuchte Lösungsanzahl ist offenbar nicht größer als die Hälfte der Lösungsanzahl r der Kongruenz

$$(47) \quad z^2 \equiv d \pmod{4k}, \quad 0 \leq z < 4k.$$

Wir setzen

$$\text{ggT}(d, 4k) =: e^2 f, \quad e, f \in \mathbb{N}, \quad f \text{ quadratfrei},$$

wodurch e und f eindeutig bestimmt sind; ferner setzen wir

$$d := e^2 f d' \quad \text{und} \quad 4k := e^2 f m .$$

Es folgt $\text{ggT}(d', m) = 1$.

Für jede Lösung z von (47) gilt $e^2 f | z^2$, also $ef | z$, da f quadratfrei ist. Sei

$$z' := \frac{z}{ef} .$$

Für dieses z sind dann mit (47) äquivalent

$$z'^2 e^2 f^2 \equiv e^2 f d' \pmod{e^2 f m}$$

und

$$z'^2 f \equiv d' \pmod{m} .$$

Sei $z' \in \mathbb{Z}$ nun eine beliebige Lösung von

$$(47') \quad z'^2 f \equiv d' \pmod{m}, \quad 0 \leq z' < m ,$$

so sind die Zahlen

$$z', z' + m, z' + 2m, \dots, z' + (e-1)m$$

alle in der gleichen Lösungsrestklasse mod m von (47').

Daher gilt:

$$efz', ef(z' + m), ef(z' + 2m), \dots, ef(z' + (e-1)m)$$

sind e Lösungen von (47), die wegen

$$0 \leq efz' < ef(z' + m) < \dots < ef(z' + (e-1)m) < efm + e^2 fm - efm \\ = 4k$$

paarweise inkongruent mod $4k$ sind. Somit folgt

$$r = er' ,$$

wobei r' die Lösungsanzahl von (47') sei.

Zur Abschätzung von r' nach oben beachten wir, daß

aus (47') im Falle der Lösbarkeit $\text{ggT}(f, m) | d'$ folgt.

Wegen $\text{ggT}(f, m) | m$ und $\text{ggT}(d', m) = 1$ ist dann $\text{ggT}(f, m) = 1$.

Sei $\bar{f} \in \mathbb{Z}$ eindeutig mod m bestimmt durch

$$\bar{f} f \equiv 1 \pmod{m} ,$$

so erhält die Kongruenz (47') die Form

$$z'^2 \equiv d' \bar{f} \pmod{m}.$$

Es gilt auch $\text{ggT}(\bar{f}, m) = 1$, also ist wegen $\text{ggT}(d', m) = 1$ dann $\text{ggT}(d' \bar{f}, m) = 1$.

Sei s die Anzahl der verschiedenen ungeraden Primteiler p von m , so folgt aus Landau [12], S. 47, Satz 88, daß wegen $m|4k$ gilt:

$$r' < 2^{s+2} < 4 \prod_{\substack{p|m \\ p \neq 2}} 2 < 4 \prod_{\substack{p|4k \\ p \neq 2}} 2 < 4 \prod_{p|k} (1 + e_p(k)) = 4 \sum_{t|k} 1 = 4\tau(k),$$

wobei $e_p(k)$ durch $p^{e_p(k)} \mid k$ und $p^{e_p(k)+1} \nmid k$ definiert ist.

Damit gilt für die Lösungsanzahl r von (47)

$$r = er' \leq \sqrt{|d|} \cdot 4\tau(k),$$

woraus nach Division durch 2 die Behauptung folgt ■

Lemma 22. Sei $2 < h_1 \in \mathbb{N}$ und $\varepsilon > 0$ beliebig.

Dann gibt es eine Konstante $C_{17} = C_{17}(h_1, \varepsilon) > 0$, so daß für alle $\vec{q} = (q_1, q_2) \in \mathbb{N}^2$, $q_1 + q_2 < h_1$ und alle $n \in \mathbb{N}$ gilt

$$\text{a) } \quad \bar{v}_2^{Q, \vec{q}}(n) < v_2^{Q, \vec{q}}(n) < C_{17} n^\varepsilon \quad \text{und}$$

$$\text{b) } \quad \bar{w}_2^{Q, \vec{q}}(n) < w_2^{Q, \vec{q}}(n) < C_{17} n^\varepsilon.$$

Beweis. Es sei $n \in \mathbb{N}$ beliebig. Da die jeweils ersten Ungleichungen in a) und b) aus der Definition der entsprechenden Ausdrücke folgen, sind nur die Anzahlen der Lösungen $(x_1, x_2) \in \mathbb{Z}^2$ von

$$q_1 x_1^2 + q_2 x_2^2 = n$$

mit den Nebenbedingungen $0 < x_1 < x_2$ bei a) und

$0 < x_1 < x_2$ für $q_1 = q_2 = 1$ bei b) in der behaupteten Weise nach oben abzuschätzen. Zu diesem Zweck lassen wir die Nebenbedingungen im folgenden unberücksichtigt.

Wir setzen $-4q_1q_2 =: d$.

Sei $k \in \mathbb{N}$. Jeder Lösung $(x, y) \in \mathbb{Z}^2$ von

$$(48) \quad q_1 x^2 + q_2 y^2 = k, \quad ggT(x, y) = 1$$

läßt sich nach Laudau[12], S. 138, Satz 201 in eindeutig bestimmter Weise eine Lösung $z \in \mathbb{Z}$ von

$$z^2 \equiv d \pmod{4k}, \quad 0 < z < 2k$$

zuordnen. ¹²⁾

Nach [12], S. 141, Satz 203 gibt es zu jedem solchen z wegen $d < -4$ höchstens 4 Lösungen von (48). Daher ist die Lösungsanzahl $\psi(k)$ von (48) nach Lemma 21 kleiner oder gleich

$$8\sqrt{|d|} \tau(k).$$

Wegen $q_1 + q_2 < h_1$ ist

$$\sqrt{|d|} = 2\sqrt{q_1q_2} < 2\sqrt{\left(\frac{h_1}{2}\right)^2} = h_1.$$

Es folgt

$$\psi(k) < 8h_1 \tau(k).$$

Sei nun $(x_1, x_2) \in \mathbb{Z}^2$ eine beliebige Lösung von

$$q_1 x_1^2 + q_2 x_2^2 = n$$

und sei $g := ggT(x_1, x_2)$, so betrachten wir

$$q_1 \left(\frac{x_1}{g}\right)^2 + q_2 \left(\frac{x_2}{g}\right)^2 = \frac{n}{g^2}.$$

In (48) sei

$$x = \frac{x_1}{g}, \quad y = \frac{x_2}{g}, \quad k = \frac{n}{g^2}.$$

¹²⁾ Die Art der Zuordnung ist a.a.O. genau beschrieben, für unseren Zweck jedoch unwichtig.

Wir erhalten nach dem eingangs Bemerkten

$$\left. \begin{array}{l} v_{2,q}^{Q(n)} \\ w_2^{Q(n)} \end{array} \right\} \leq \sum_{g^2|n} \psi\left(\frac{n}{g^2}\right) \leq 8h_1 \sum_{g^2|n} \tau\left(\frac{n}{g^2}\right) \leq 8h_1 \sum_{g|n} \tau(n) = 8h_1 \tau^2(n).$$

Bekanntlich gibt es zu jedem $\varepsilon > 0$ eine von n unabhängige Konstante $C_{18} > 0$ mit

$$\tau(n) \leq C_{18} n^{\varepsilon/2}.$$

(Siehe z.B. Hardy und Wright [10], S. 260, Satz 315.)

Mit $c_{17} := 8h_1 C_{18}$ folgen die Behauptungen a) und b) ■

Aus Ergebnissen von Siegel [19] und Bateman [1] folgt

Lemma 23. Zu jedem $\varepsilon > 0$ gibt es eine Konstante $C_{19} > 0$,
so daß für jedes $n \in \mathbb{N}$, $n \neq 0$, 4 und 7 (mod 8) gilt

$$w_3^{Q(n)} > C_{19} n^{\frac{1}{2} - \varepsilon}.$$

Beweis. Sei $n \in \mathbb{N}$. Die Formel von Bateman [1] über die Anzahl $r_3(n)$ der Darstellungen $(x_1, x_2, x_3) \in \mathbb{Z}^3$ von n durch die Form

$$x_1^2 + x_2^2 + x_3^2$$

(wobei also Vorzeichen und Reihenfolge der Summanden berücksichtigt werden) lautet

$$(49) \quad r_3(n) = \frac{16}{\pi} n^{1/2} \chi_2(n) K(-4n) \prod_{p^2|n} \left(1 + \frac{1}{p} + \dots + \frac{1}{p^{b-1}} + \frac{1}{p^b} \left(1 - \left(\frac{-p^{-2b}n}{p} \right) \frac{1}{p} \right)^{-1} \right),$$

wobei $b=b(p)$ die größte ganze Zahl ist, für die gilt $p^{2b}|n$.

Ferner ist

$$K(-4n) := \sum_{m=1}^{\infty} \left(\frac{-4n}{m} \right) \frac{1}{m} .$$

Ist 4^w die höchste Potenz von 4, die n teilt, dann ist

$$(50) \quad \chi_2(n) := \begin{cases} 0 & \text{falls } 4^{-w}n \equiv 7 \pmod{8} \\ \frac{1}{2^w} & \text{falls } 4^{-w}n \equiv 3 \pmod{8} \\ \frac{3}{2^{w+1}} & \text{falls } 4^{-w}n \equiv 1, 2, 5 \text{ oder } 6 \pmod{8} \end{cases}$$

Siegel [19] hat für jedes $\varepsilon_1 > 0$ gezeigt, daß es ein

$C_{20} = C_{20}(\varepsilon_1) > 0$ gibt mit

$$(51) \quad K(d) := \sum_{m=1}^{\infty} \left(\frac{d}{m} \right) \frac{1}{m} > C_{20} |d|^{-\varepsilon_1}$$

für alle Fundamentaldiskriminanten d ; d.h. für alle $d \in \mathbb{Z}$ mit $d \equiv 0$ oder $1 \pmod{4}$, d kein Quadrat, durch kein Quadrat einer ungeraden Primzahl teilbar und entweder ungerade oder $\equiv 8$ oder $12 \pmod{16}$.

Zu n gibt es ein $z \in \mathbb{N}$ und eine Fundamentaldiskriminante d , so daß gilt

$$(52) \quad -4n = z^2 d$$

und

$$(53) \quad K(-4n) = \prod_{\substack{p|z \\ p \text{ Primz.}}} \left(1 - \left(\frac{d}{p} \right) \frac{1}{p} \right) \cdot K(d)$$

(siehe z.B. Landau [12], S. 172, Satz 214).

Es gilt (siehe Hardy und Wright [10], S.267, Satz 328)

$$\lim_{m \rightarrow \infty} \frac{\varphi(m) \log \log m}{m} = e^{-\gamma} ,$$

wobei $\gamma = 0,57721\dots$ die Eulersche Konstante ist.

Wegen $\frac{\varphi(m) \log \log m}{m} > 0$ für $m > 3$ gilt für ein $0 < C_{21} < e^{-\gamma}$

und alle $m \geq m_0$, daß

$$\frac{\varphi(m)}{m} > C_{21} (\log \log m)^{-1}.$$

Damit folgt aus (53), (52) und (51) mit $\varepsilon_1 := \frac{\varepsilon}{2}$ für

$4n \geq m_0$, daß

$$\begin{aligned} K(-4n) &> \prod_{\substack{p|4n \\ p \text{ Primz.}}} \left(1 - \frac{1}{p}\right) \cdot K(d) \\ &> \frac{\varphi(4n)}{4n} \cdot C_{20} |d|^{-\varepsilon/2} \\ &> C_{21} (\log \log 4n)^{-1} \cdot C_{20} (4n)^{-\varepsilon/2} \\ &> n^{-\varepsilon} \quad \text{für alle } n \geq n_1. \end{aligned}$$

Für ein geeignetes $0 < C_{22} < 1$ gilt dann

$$(54) \quad K(-4n) > C_{22} n^{-\varepsilon} \quad \text{für alle } n \in \mathbb{N}.$$

Nun ist $n \not\equiv 0, 4$ und $7 \pmod{8}$. Daher folgt wegen (50)

und (54) aus (49), daß

$$(55) \quad r_3(n) > \frac{16}{\pi} n^{1/2} \cdot \frac{3}{2} C_{22} n^{-\varepsilon}.$$

Zu einer Darstellung $(x_1, x_2, x_3) \in \mathbb{N}^3$ von n mit

$$(56) \quad n = x_1^2 + x_2^2 + x_3^2$$

und

$$0 \leq x_1 \leq x_2 \leq x_3,$$

die in $w_3^Q(n)$ gezählt wird, gibt es insgesamt höchstens

6 Darstellungen, die durch Permutation der x_i^2 ($i=1,2,3$)

in (56) entstehen; zu jeder davon wiederum höchstens 8,

die durch die Kombinationen der Vorzeichen in

$$n = (\pm x_1)^2 + (\pm x_2)^2 + (\pm x_3)^2$$

gebildet werden können.

Mit (55) folgt

$$w_3^Q(n) > \frac{r_3(n)}{6 \cdot 8} > \frac{1}{2\pi} C_{22} n^{1/2-\varepsilon} =: C_{19} n^{1/2-\varepsilon} \quad \blacksquare$$

Lemma 24. Sei $h=3$ oder $h=4$, $A_h \subseteq \mathbb{Q}$ und $M_h \subseteq \mathbb{N}$ mit

$$(57) \quad \{m \in \mathbb{N} \mid m \equiv 2 \pmod{4}\} \subseteq M_h \subseteq h \cdot A_h.$$

Für $C_3^{(h)} > 0$ und $c' > 0$ gelte

$$(58) \quad A_h(n) \leq C_3^{(h)} n^{\frac{1}{h} + c'} \quad \text{für alle } n \in \mathbb{N}.$$

Sei

$$(59) \quad G_h := \{g^2 \in A_h \mid g \equiv 0 \pmod{2}\}$$

und

$$(60) \quad U_h := \{u^2 \in A_h \mid u \equiv 1 \pmod{2}\}.$$

Dann gilt für Konstante $C_{23}^{(h)} > 0$ und $C_{24}^{(h)} > 0$,

daß

$$G_h(n) \geq C_{23}^{(h)} n^{\frac{1}{h} - \frac{2c'}{h-2}} \quad \text{für alle } n \in \mathbb{N}, n \geq 4$$

und

$$U_h(n) \geq C_{24}^{(h)} n^{\frac{1}{h} - \frac{h-2}{2} c'} \quad \text{für alle } n \in \mathbb{N}.$$

Beweis. Es gibt ein $C_{25} > \max(C_3^{(3)}, C_3^{(4)})$, so daß für alle $n \in \mathbb{N}$ gilt

$$(61) \quad G_h(n) + 1 \leq A_h(n) + 1 \leq C_{25} n^{\frac{1}{h} + c'}$$

und

$$(62) \quad U_h(n) + 1 \leq A_h(n) + 1 \leq C_{25} n^{\frac{1}{h} + c'}$$

Sei $m \equiv 2 \pmod{4}$, dann kann wegen $h=3$ oder $h=4$ die Zahl m nur in der Form

$$m = u_1^2 + u_2^2 + \sum_{i=1}^{h-2} g_i^2$$

mit $u_1, u_2 \in U_h$ und $g_i \in G_h \cup \{0\}$ für $1 \leq i \leq h-2$ dargestellt werden, wenn man von der Reihenfolge der Summanden absieht.

Also gilt wegen (57):

$$\{m \in \mathbb{N} \mid m \equiv 2 \pmod{4}\} \subseteq 2 U_h + (h-2)(G_h \cup \{0\}).$$

Die Anzahl der $m \equiv 2 \pmod{4}$ mit $m \leq n$ ist kleiner oder gleich $\frac{n}{4}$. Aus Lemma 20 folgt

$$(63) \quad \frac{n}{4} \leq (U_h(n) + 1)^2 (G_h(n) + 1)^{h-2} \quad \text{für alle } n \in \mathbb{N}.$$

Mit (62) erhalten wir für alle $n \in \mathbb{N}$

$$\begin{aligned} G_h(n) &> \left(\frac{n}{4(U_h(n) + 1)^2} \right)^{\frac{1}{h-2}} - 1 \\ &> \left(\frac{n}{4 C_{25}^2 n^{\frac{2}{h} + 2c'}} \right)^{\frac{1}{h-2}} - 1 \\ &= (4 C_{25}^2)^{-\frac{1}{h-2}} n^{\left(1 - \frac{2}{h} - 2c'\right) \frac{1}{h-2}} - 1 \\ &= (2 C_{25})^{-\frac{2}{h-2}} n^{\frac{1}{h} - \frac{2c'}{h-2}} - 1. \end{aligned}$$

Wegen (57) ist $2^2 \in A_h$, also $2^2 \in G_h$. Dann gibt es ein C_{26}

mit $(2 C_{25})^{-\frac{2}{h-2}} > C_{26} > 0$, so daß

$$G_h(n) > C_{26} n^{\frac{1}{h} - \frac{2c'}{h-2}} \quad \text{für alle } n \in \mathbb{N}, n > 4.$$

Wegen (63) und (61) gilt für alle $n \in \mathbb{N}$

$$\begin{aligned} U_h(n) &> \left(\frac{n}{4(G_h(n) + 1)^{h-2}} \right)^{1/2} - 1 \\ &> \left(\frac{n}{4 C_{25}^{h-2} n^{\frac{h-2}{h} + (h-2)c'}} \right)^{1/2} - 1 \\ &= \frac{1}{2} C_{25}^{-\frac{h-2}{2}} n^{\frac{1}{h} - \frac{h-2}{2} c'} - 1. \end{aligned}$$

Wegen (57) ist $1^2 \in A_h$, also $1^2 \in U_h$. Dann gibt es ein C_{27}

mit $C_{25}^{-\frac{h-2}{2}} > C_{27} > 0$, so daß

$$U_h(n) \geq C_{27} n^{\frac{1}{h} - \frac{h-2}{2} C}, \quad \text{für alle } n \in \mathbb{N} \quad \blacksquare$$

3.7 Wir beweisen nun Satz 4 in der folgenden Fassung

Lemma 25. Sei $\varepsilon > 0$, $h_1 \in \mathbb{N}$, $4 \leq h_1$ und $h \in \mathbb{N}$, $3 \leq h \leq h_1$.

Dann gibt es Mengen $A_h = A_{h,\varepsilon} \subseteq \mathbb{N}$ für $h=3,4,\dots,h_1$
mit $Q \supseteq A_3 \supseteq A_4 \supseteq \dots \supseteq A_{h_1}$ und

$$(64^{(h)}) \quad M_h \subseteq h \circ A_h \quad \text{für } h=3,4,\dots,h_1,$$

wobei

$$(65) \quad M_h = \begin{cases} \{n \in \mathbb{N} \mid n \not\equiv 0, 4 \text{ und } 7 \pmod{8}\} & \text{für } h=3 \\ \{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\} & \text{für } h=4, \\ \mathbb{N} & \text{für } h \geq 5 \end{cases}$$

und es gibt Konstante $C_3^{(h)} = C_3(\varepsilon, h_1, h) > 0$ und
 $C_{14}^{(h)} = C_{14}(\varepsilon, h_1, h) > 0$, so daß für alle $n \in \mathbb{N}$ gilt

$$(32^{(h)}) \quad A_h(n) \leq C_3^{(h)} n^{\frac{1}{h} + \varepsilon \cdot 9^{h-h_1}} \quad 13)$$

$$(33^{(h)}) \quad w_h A_h(n) \leq C_{14}^{(h)} n^{\varepsilon \cdot 9^{h-h_1}}.$$

13) Für $h=3$ ist $(32^{(h)})$ bereits von Erdős und Nathanson [7] bewiesen worden. Dieses Ergebnis kann hier jedoch nicht herangezogen werden, da die Existenz der Menge A_3 mit $(32^{(3)})$ im Zusammenhang mit $(33^{(3)})$ zu zeigen ist (siehe Beweise von Satz 8 und Lemma 18).

Satz 4 ergibt sich aus Lemma 25 mit $h=h_1$ und $B_{h,\varepsilon} = A_{h,\varepsilon} \cup \{0\}$.

Beweis von Lemma 25 (durch Induktion nach h).

O.B.d.A. sei

$$\varepsilon < \frac{1}{h_1-1}$$

Es folgt für $1 \leq h \leq h_1$

$$(66) \quad \varepsilon \cdot 9^{h-1-h_1} < \frac{9^{h-h_1}}{9(h_1-1)} < \frac{1}{5(h-1)}.$$

$h=3$:

Zur Anwendung von Lemma 18 wählen wir h_1 wie in der Voraussetzung, $h:=3$, $A:=Q$ und

$$c = c^{(2)} := \varepsilon \cdot 9^{2-h_1}.$$

Nach Satz 2 gilt für $M_3 = \{n \in \mathbb{N} \mid n \neq 0, 4 \text{ und } 7 \pmod{8}\}$, daß $M_3 \subseteq 3 \circ Q$. Daher kann man in Lemma 18 die Menge $M=M_3$ wählen. (30) folgt aus (66) und (31) aus Lemma 23. Wegen

$$Q(n) \leq n^{1/2} \leq n^{1/2+c} \quad \text{für alle } n \in \mathbb{N}$$

gilt (32), während (33), (34) und (35) für $k=2$ nach Lemma 22 für alle $n \in \mathbb{N}$ und alle $\vec{q} = (q_1, q_2) \in \mathbb{N}^2$, $q_1+q_2 \leq h_1$ erfüllt sind. Für $k=1$ gilt (35) trivialerweise.

Nach Lemma 18 gibt es daher eine Menge $A_3 := A' \subseteq Q$ mit

$$(64^{(3)}) \quad M_3 \subseteq 3 \circ A_3$$

und Konstante $C_i^{(3)} = C_i^{(3)}(\varepsilon, h_1) > 0$ ($i=3, 14, 6, 15$) so daß mit der Bezeichnung

$$H_1^{(j)} := \{(q_1, q_2, \dots, q_j) \in \mathbb{N}^j \mid q_1+q_2+\dots+q_j \leq h_1\}$$

für alle $n \in \mathbb{N}$ gilt:

$$(32^{(3)}) \quad A_3(n) \leq C_3^{(3)} n^{\frac{1}{3} + 3\varepsilon \cdot 9^{2-h_1}} \leq C_3^{(3)} n^{\frac{1}{3} + \varepsilon \cdot 9^{3-h_1}},$$

$$(33^{(3)}) \quad w_3 A_3(n) \leq C_{14}^{(3)} n^{\varepsilon \cdot 9^{3-h_1}},$$

$$(34^{(3)}) \quad v_{3,\bar{q}} A_3(n) \leq C_6^{(3)} n^{\varepsilon \cdot 9^{3-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(3)} \text{ und}$$

$$(35^{(3)}) \quad \bar{v}_{3,\bar{q}} A_3(n) \leq C_{15}^{(3)} n^{\varepsilon \cdot 9^{3-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(k)} \\ k=1,2,3.$$

Durch $(32^{(3)})$ und $(33^{(3)})$ ist die Behauptung für $h=3$ nachgewiesen. Um Lemma 18 später mit $h=4$ anwenden zu können, fehlt noch die dortige Voraussetzung (31), die wir nun herleiten. Sei zunächst weiterhin $h=3$.

Zur Anwendung von Lemma 24 behalten die dort auftretenden Mengen A_3 und M_3 ihre Bezeichnung bei; ebenso die Größen $h=3$ und $C_3^{(3)}$ (wie in $(32^{(3)})$). Es sei $c' := 3\varepsilon \cdot 9^{2-h_1}$. Wegen $M_3 \subseteq 3 \cdot A_3$ ist insbesondere (57) erfüllt. (58) gilt wegen der ersten Ungleichung in $(32^{(3)})$. Für die in (59) und (60) definierten Mengen

$$G_3 := \{g^2 \in A_3 \mid g \equiv 0 \pmod{2}\}$$

und

$$U_3 := \{u^2 \in A_3 \mid u \equiv 1 \pmod{2}\}$$

gilt daher mit Konstanten $C_{23}^{(3)} > 0$ und $C_{24}^{(3)} > 0$

$$(67) \quad G_3(n) \geq C_{23}^{(3)} n^{\frac{1}{3} - 6\varepsilon \cdot 9^{2-h_1}} \quad \text{für alle } n \in \mathbb{N}, n \geq 4$$

und

$$(68) \quad U_3(n) \geq C_{24}^{(3)} n^{\frac{1}{3} - \frac{3}{2}\varepsilon \cdot 9^{2-h_1}} \quad \text{für alle } n \in \mathbb{N}.$$

Sei nun $n \in M_4 = \{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\}$, $n > 1$.

Wir unterscheiden vier Fälle:

$n \equiv 1 \pmod{4}$:

Für jedes $b^2 \in G_3$ mit $b^2 \leq n$ gilt

$$n - b^2 \equiv 1 \pmod{4}.$$

Wegen $n > 1$ ist $n > 5$, also gibt es nach (67) min-

destens $C_{23}^{(3)} n^{\frac{1}{3} - 6\epsilon \cdot 9^{2-h_1}}$ solcher $b^2 \in G_3 \subseteq A_3$.

$n \equiv 2 \pmod{4}$:

Für jedes $b^2 \in A_3$ mit $b^2 \leq n$ ist

$$n - b^2 \equiv 1 \text{ oder } 2 \pmod{4}$$

und es gibt wegen $A_3 \supseteq U_3$ mindestens $U_3(n)$ solcher $b^2 \in A_3$.

$n \equiv 3 \pmod{4}$:

Für jedes $b^2 \in U_3$ mit $b^2 \leq n$ ist

$$n - b^2 \equiv 2 \pmod{4}$$

und es gibt $U_3(n)$ solcher $b^2 \in U_3 \subseteq A_3$.

$n \equiv 4 \pmod{8}$:

Für jedes $b^2 \in U_3$ mit $b^2 \leq n$ ist

$$n - b^2 \equiv 3 \pmod{8}$$

und es gibt $U_3(n)$ solcher $b^2 \in U_3 \subseteq A_3$.

In den letzten drei Fällen gibt es nach (68) also jeweils

mindestens $C_{24}^{(3)} n^{\frac{1}{3} - \frac{3}{2}\epsilon \cdot 9^{2-h_1}}$ verschiedene $b^2 \in A_3$ mit $b^2 \leq n$ und $n - b^2 \not\equiv 0, 4 \text{ und } 7 \pmod{8}$.

Sei $C_{28} := \min(C_{23}^{(3)}, C_{24}^{(3)})$, so folgt insgesamt aus der obigen Fallunterscheidung:

Zu jedem $n \in M_4 = \{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\}$, $n > 1$ gibt es mindestens

$$(69) \quad C_{28} n^{\frac{1}{3} - 6\epsilon \cdot 9^{2-h}}$$

verschiedene $b^2 \in A_3$ mit $b^2 \leq n$, so daß gilt

$$n - b^2 \equiv 0, 4 \text{ und } 7 \pmod{8},$$

also $0 < n - b^2 \in M_3$. Wegen $M_3 \subseteq 3 \circ A_3$ ist daher $n - b^2$ Summe von höchstens 3 Quadraten aus A_3 . Lemma 19a) liefert

wegen (69) mit $h = 4$, $m = C_{28} \frac{1}{3} - 6\varepsilon \cdot 9^{2-h_1}$ und $A = A_3$ nun

$$w_4^{A_3}(n) \geq \frac{A_3(n)}{4} \geq \frac{C_{28}}{4} n^{\frac{1}{3} - 6\varepsilon \cdot 9^{2-h_1}} \geq \frac{C_{28}}{4} n^{\frac{1}{3} - \varepsilon \cdot 9^{3-h_1}}.$$

Da $1 \in M_3 \subseteq 3 \circ A_3$ folgt $1 \in A_3$, also $w_4^{A_3}(1) = 1$. Daher gilt

mit $C_{13}^{(3)} := \min(1, \frac{C_{28}}{4})$

$$(31^{(3)}) \quad w_4^{A_3}(n) \geq C_{13}^{(3)} n^{\frac{1}{3} - \varepsilon \cdot 9^{3-h_1}} \quad \text{für alle } n \in M_4.$$

Insbesondere gilt

$$M_4 \subseteq 4 \circ A_3.$$

$h = 4$:

Wieder wenden wir Lemma 18 an mit h_1 wie in der Voraussetzung, $h=4$, $A=A_3$ und

$$c := \varepsilon \cdot 9^{3-h_1}.$$

(30) gilt wegen (66) und (31) bis (35) gelten wegen

(31⁽³⁾) bis (35⁽³⁾). Es gibt daher eine Menge $A_4 \subseteq A_3$ mit

$$(64^{(4)}) \quad M_4 \subseteq 4 \circ A_4$$

und Konstante $C_i^{(4)} = C_i^{(4)}(\varepsilon, h_1) > 0$ ($i = 3, 14, 6, 15$), so

daß für alle $n \in \mathbb{N}$ gilt:

$$(32^{(4)}) \quad A_4(n) \leq C_3^{(4)} n^{\frac{1}{4} + 3\varepsilon \cdot 9^{3-h_1}} \leq C_3^{(4)} n^{\frac{1}{4} + \varepsilon \cdot 9^{4-h_1}},$$

$$(33^{(4)}) \quad w_4^{A_4}(n) \leq C_{14}^{(4)} n^{\varepsilon \cdot 9^{4-h_1}},$$

$$(34^{(4)}) \quad v_{4,\bar{q}}^{A_4}(n) \leq C_6^{(4)} n^{\varepsilon \cdot 9^{4-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(4)} \text{ und}$$

$$(35^{(4)}) \quad \bar{v}_{h,\bar{q}}^{A_4}(n) < C_{15}^{(4)} n^{\varepsilon \cdot 9^{4-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(k)},$$

$k=1,2,3,4.$

Damit ist die Behauptung auch für $h=4$ gezeigt.

Mit den Werten $h=4$, $c'=3\varepsilon \cdot 9^{3-h_1}$, $C_3^{(4)}$ und den Mengen A_4 und M_4 wenden wir wieder Lemma 24 an und erhalten für Konstante $C_{23}^{(4)} > 0$ und $C_{24}^{(4)} > 0$ aus (32⁽⁴⁾) nun

$$(70) \quad G_4(n) \geq C_{23}^{(4)} n^{\frac{1}{4} - 3\varepsilon \cdot 9^{3-h_1}} \quad \text{für alle } n \in \mathbb{N}, n \geq 4$$

und

$$(71) \quad U_4(n) \geq C_{24}^{(4)} n^{\frac{1}{4} - 3\varepsilon \cdot 9^{3-h_1}} \quad \text{für alle } n \in \mathbb{N},$$

wobei G_4 bzw. U_4 wiederum die geraden bzw. ungeraden Quadrate aus A_4 sind.

Für $n \in M_5 = \mathbb{N}$, $n > 3$ unterscheiden wir zwei Fälle:

$n \equiv 1 \pmod{2}$:

Für jedes $b^2 \in G_4 \subseteq A_4$ mit $b^2 \leq n$ ist

$$n - b^2 \equiv 1 \pmod{2}.$$

Wegen $n > 3$ ist $n \geq 5$, also gibt es nach (70) mindestens

$$C_{23}^{(4)} n^{\frac{1}{4} - 3\varepsilon \cdot 9^{3-h_1}} \quad \text{solcher } b^2 \in G_4.$$

$n \equiv 0 \pmod{2}$:

Für jedes $b^2 \in U_4 \subseteq A_4$ mit $b^2 \leq n$ ist

$$n - b^2 \equiv 1 \pmod{2}.$$

Nach (71) gibt es mindestens $C_{24}^{(4)} n^{\frac{1}{4} - 3\varepsilon \cdot 9^{3-h_1}}$ solcher $b^2 \in U_4$.

Sei $C_{29} := \min(1, C_{23}^{(4)}, C_{24}^{(4)})$. Nach dem soeben Gezeigten gibt es dann zu jedem $n \in \mathbb{N} = M_5$, $n > 3$ mindestens

$$C_{29} n^{\frac{1}{4} - 3\epsilon \cdot 9^{3-h_1}}$$

verschiedene $b^2 \in A_4$, $b^2 \leq n$ mit $n - b^2 \equiv 1 \pmod{2}$, woraus

$0 < n - b^2 \in \{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\} = M_4$ folgt. Wegen $M_4 \subseteq 4 \circ A_4$

ist also $n - b^2$ Summe von höchstens 4 Quadraten aus A_4 .

Lemma 19a) liefert dann mit $C_{13}^{(4)} := \frac{C_{25}}{5}$

$$(31^{(4)}) \quad w_5^{A_4}(n) \geq \frac{C_{29}}{5} n^{\frac{1}{4} - 3\epsilon \cdot 9^{3-h_1}} \geq C_{13}^{(4)} n^{\frac{1}{4} - \epsilon \cdot 9^{3-h_1}}$$

für alle $n \in \mathbb{N} = M_5$, denn für $n=1,2,3$ ist $w_5^{A_4}(n) = 1$, da

$1 \in A_4$; außerdem ist $C_{13}^{(4)} = \frac{C_{29}}{5} \leq \frac{1}{5} < 3^{-1/4}$. Insbesondere

ist $M_5 = \mathbb{N} = 5 \circ A_4$.

Alle Voraussetzungen von Lemma 18 für $h=5$, $A:=A_4$,

$c := \epsilon \cdot 9^{4-h_1}$ und $M := M_5 = \mathbb{N}$ sind mit (66) und (31⁽⁴⁾) bis

(35⁽⁴⁾) wiederum erfüllt.

$h-1 \Rightarrow h$, wobei $5 \leq h \leq h_1$:

Die Voraussetzungen von Lemma 18 seien mit h , $A := A_{h-1}$,

$c := \epsilon \cdot 9^{h-1-h_1}$, $M := M_h = \mathbb{N} = h \circ A_{h-1}$ erfüllt.

Dann folgt aus Lemma 18 die Existenz von Konstanten

$C_i^{(h)} := C'_i > 0$ ($i=3, 14, 6, 15$) und einer Menge $A_h \subseteq A_{h-1}$

mit

$$(64^{(h)}) \quad M_h = \mathbb{N} = h \circ A_h$$

und den Eigenschaften

$$(32^{(h)}) \quad A_h(n) \leq C_3^{(h)} n^{\frac{1}{h} + 3\epsilon \cdot 9^{h-1-h_1}} \leq C_3^{(h)} n^{\frac{1}{h} + \epsilon \cdot 9^{h-h_1}}$$

$$(33^{(h)}) \quad w_h^{A_h(n)} < C_{14}^{(h)} n^{\varepsilon \cdot 9^{h-h_1}}$$

$$(34^{(h)}) \quad v_{h,\bar{q}}^{A_h(n)} < C_6^{(h)} n^{\varepsilon \cdot 9^{h-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(h)} \text{ und}$$

$$(35^{(h)}) \quad \bar{v}_{k,\bar{q}}^{A_h(n)} < C_{15}^{(h)} n^{\varepsilon \cdot 9^{h-h_1}} \quad \text{für alle } \bar{q} \in H_1^{(k)}, \\ k=1,2,\dots,h$$

jeweils für alle $n \in \mathbb{N}$.

Für $h < h_1$ ist noch $(31^{(h)})$ zu zeigen:

Wegen $(64^{(h)})$ ist $A_h \cup \{0\}$ Basis der Ordnung h . Nach Lemma 20 ist für ein $C_{16}^{(h)} > 0$

$$A_h(n) > C_{16}^{(h)} n^{\frac{1}{h}} \quad \text{für alle } n \in \mathbb{N}.$$

Aus Lemma 19b) folgt wegen $\mathbb{N} = h \circ A_h$ für alle $n \in \mathbb{N}$, daß

$$w_{h+1}^{A_h(n)} > \frac{A_h(n)}{h+1} > \frac{C_{16}^{(h)}}{h+1} n^{\frac{1}{h}} =: C_{13}^{(h)} n^{\frac{1}{h}},$$

also insbesondere

$$(31^{(h)}) \quad w_{h+1}^{A_h(n)} > C_{13}^{(h)} n^{\frac{1}{h} - \varepsilon \cdot 9^{h-h_1}} \quad \text{für alle } n \in \mathbb{N}$$

und

$$M_{h+1} = \mathbb{N} = (h+1) \circ A_h.$$

Damit ist Lemma 18 wieder anwendbar. Nach insgesamt

$h_1 - 4$ Schritten sind $(64^{(h)})$ mit (65) , sowie $(32^{(h)})$ und $(33^{(h)})$ für $h=3,4,\dots,h_1$ gezeigt ■

Beweis von Satz 5. Nach Satz 4 gibt es zu jedem $\varepsilon > 0$

eine Basis $B_{4, \varepsilon/2}$ der Ordnung 4 für $M_4 = \{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{8}\}$

und eine Konstante $C_1 = C_1(4, \varepsilon/2) > 0$, so daß gilt

$$(72) \quad B_{4, \varepsilon/2}(n) \leq C_1 n^{1/4 + \varepsilon/2} \quad \text{für alle } n \in \mathbb{N}.$$

Es sei

$$B_\varepsilon := \{(2^k b)^2 \mid b^2 \in B_{4, \varepsilon/2}, k \in \mathbb{N}_0\}.$$

Ist $n_1 \in \mathbb{N}$ beliebig, so gibt es ein $m \in M_4$ und ein $k \in \mathbb{N}_0$ mit $n_1 = 4^k m$. Wegen

$$m = b_1^2 + b_2^2 + b_3^2 + b_4^2, \quad b_i^2 \in B_{4, \varepsilon/2}, \quad i=1,2,3,4$$

folgt

$$n_1 = (2^k b_1)^2 + (2^k b_2)^2 + (2^k b_3)^2 + (2^k b_4)^2.$$

Also ist B_ε eine Basis der Ordnung 4 für $\mathbb{N}$.

Sei nun $n \in \mathbb{N}$ beliebig. Für jedes $b \in B_{4, \varepsilon/2}$, $b \geq 1$ folgt aus $(2^k b)^2 \leq n$, daß

$$0 \leq k \leq \frac{\log \sqrt{n}}{\log 2}.$$

Daher gibt es zu jedem $b \in B_{4, \varepsilon/2}$, $b \geq 1$ höchstens $1 + \frac{\log \sqrt{n}}{\log 2}$ Quadrate $(2^k b)^2$ in B_ε , die nicht größer als n sind. Aus (72) folgt mit einem geeigneten $C > 0$, daß

$$B(n) \leq (1 + \frac{\log \sqrt{n}}{\log 2}) B_{4, \varepsilon/2}(n) \leq (1 + \frac{\log \sqrt{n}}{\log 2}) C_1 n^{1/4 + \varepsilon/2} \leq C n^{1/4 + \varepsilon}$$

für alle $n \in \mathbb{N}$ ■

3.8 Mit Satz 5 ist auch ein Problem von Choi, Erdős

und Nathanson [2] gelöst. Dort wird vermutet, daß es für jedes $\varepsilon > 0$ und alle genügend großen $n \in \mathbb{N}$ eine endliche Menge A von Quadraten gibt, so daß gilt

$$|A| \leq n^{1/4 + \varepsilon},$$

und jedes $m = 1, 2, \dots, n$ ist Summe von 4 Quadraten aus A .¹⁴⁾

¹⁴⁾ In [25] wurde ein Beweis dieser Aussage angegeben, der auf einem Ergebnis von Erdős und Nathanson [7] (Theorem 3) basiert.

A ist daher Abschnittsbasis der Ordnung 4 für $[1, h]$.

Aus Satz 4 und Satz 5 folgt der allgemeinere

Satz 9. Zu jedem $h \in \mathbb{N}$, $h \geq 4$, jedem $\varepsilon > 0$ und jedem $n > n_0(h, \varepsilon)$ gibt es eine endliche Menge A von Quadraten, so daß

$$|A| < n^{1/h + \varepsilon},$$

und jedes $m = 1, 2, \dots, n$ ist Summe von h Quadraten aus A.

Beweis. Sei $h \geq 4$. Nach Satz 4 bzw. Satz 5 gibt es zu jedem $\varepsilon > 0$ eine Basis h-ter Ordnung $\tilde{B}_{h, \varepsilon/2} := B_{h, \varepsilon/2}$ für $h \geq 5$, bzw. $\tilde{B}_{h, \varepsilon/2} := B_{\varepsilon/2}$ für $h=4$, die nur aus Quadraten besteht und eine Konstante $\tilde{C} = \tilde{C}(h, \varepsilon) > C_1(h, \varepsilon/2)$ bzw. $\tilde{C} > C(\varepsilon/2)$ mit

$$(73) \quad 1 + \tilde{B}_{h, \varepsilon/2}(n) < \tilde{C} n^{1/2 + \varepsilon/2} \quad \text{für alle } n \in \mathbb{N}.$$

Es gibt ein $n_0 = n_0(h, \varepsilon) \in \mathbb{N}$, so daß für alle $n > n_0$ gilt

$$(74) \quad \tilde{C} < n^{\varepsilon/2}.$$

Wir wählen $A := \tilde{B}_{h, \varepsilon/2} \cap [0, n]$. Es folgt

$$\{0, n\} \subseteq hA$$

und mit (73) und (74)

$$|A| = 1 + \tilde{B}_{h, \varepsilon/2}(n) < \tilde{C} n^{1/h + \varepsilon/2} < n^{1/h + \varepsilon} \quad \text{für alle } n > n_0 \quad \blacksquare$$

3.9 Könnte die Ungleichung (51) von Siegel (siehe Beweis von Lemma 22) verschärft werden, so würde sich dies nach einigen Modifikationen in den Beweisen der Lemmata 10, 13, 14, 18 und 22 bis 25 sowie des Satzes 8 in entsprechender Weise auf die Ungleichungen in Satz 4 und Satz 5 auswirken, wobei man mit dem hier eingeschlagenen

Weg jedoch höchstens

$$B_{h,c}(n) < C'_1 n^{\frac{1}{h}} e^{\frac{c \log n}{\log \log n}}$$

und

$$w_h^{B_{h,c}}(n) < C'_2 n^{\frac{1}{h}} e^{\frac{c \log n}{\log \log n}}$$

erreichen könnte für beliebig vorgegebenes $c > 0$.

3.10 Es folgen nun noch einige Bemerkungen zu den in diesem Paragraphen auftretenden Konstanten.

Die in Lemma 10 bei E' und in Lemma 14 bei $E''_{\frac{q}{q}}$ vorkommenden endlichen Ausnahmemengen (bei E' als F bezeichnet) ergeben sich aus dem Lemma von Borel - Cantelli.

Daraus erhält man jedoch keinen Hinweis auf die Elementanzahlen dieser Ausnahmemengen. Die Konstanten C_{10} und C_{11} in Satz 8 und auch die Konstanten C_1 , C_2 und C in den Sätzen 4 und 5 sind darum nicht effektiv (s. Beweis von Satz 8). Folgendes läßt sich jedoch zeigen:

Für die in Satz 4 angegebene Menge $B_{h,\varepsilon}$ der Ordnung h gilt für ein ε' mit $0 < \varepsilon' < \varepsilon$

$$B_{h,\varepsilon}(n) \sim C'_{h,\varepsilon} n^{\frac{1}{h} + \varepsilon'} \quad \text{für } n \rightarrow \infty.$$

Für jedes feste h gilt

$$C'_{h,\varepsilon} \rightarrow h^{\frac{h}{4}} \sqrt{\frac{h}{4h!}} < 2,724 \quad , \text{ wenn } \varepsilon \rightarrow 0.$$

In dem wichtigen Fall $h=4$ sei die Abhängigkeit der Konstanten $C'_{4,\varepsilon}$ von ε genauer angegeben:

Für die in Satz 4 angegebene Basis $B_{4,\varepsilon}$ der Ordnung 4 für $\{n \in \mathbb{N} | n \not\equiv 0 \pmod{8}\}$ gilt mit

$$\varepsilon' = \frac{\varepsilon}{2} \cdot \frac{90 + 11\varepsilon}{243 + 87\varepsilon + 2\varepsilon^2} < \frac{\varepsilon}{5}, \text{ da\ss}$$

$$B_{4,\varepsilon}(n) \sim C_{4,\varepsilon}' n^{1/4 + \varepsilon'} \quad \text{für } n \rightarrow \infty, \text{ wobei}$$

$$C_{4,\varepsilon}' = \frac{4}{3} \cdot \frac{1 + \varepsilon/3}{1 + \varepsilon} \cdot \left(\frac{3}{2} \cdot \frac{1 + 2\varepsilon/81}{1 + 8\varepsilon/81} \right)^{\frac{3}{4} \cdot \frac{1 + \varepsilon}{1 + \varepsilon/3}}.$$

Daher gilt

$$C_{4,\varepsilon}' \rightarrow \frac{4}{3} \left(\frac{3}{2} \right)^{3/4} = 1,807... \quad \text{für } \varepsilon \rightarrow 0.$$

$$(\text{Z.B. ist } C_{4,1/1000}' = 1,806...)$$

Zum Beweis dieser Aussagen erinnern wir an die im Beweis von Satz 8 getroffenen Festlegungen. Für den dort betrachteten Wahrscheinlichkeitsraum (X, S, P) mit $P(B^{(n)}) = p(n) = n^{-s}$ für alle $n \in \mathbb{N}$ ist

$$(75) \quad s = \frac{b}{ah} - \frac{a-b}{ah} = \frac{1}{ah}(2b-a).$$

Wegen $\frac{a}{2} < b < a$ und $h \in \mathbb{N}$ folgt daraus

$$0 < s = \frac{1}{ah}(2b-a) < \frac{1}{ah}(2a-a) = \frac{1}{h} < 1.$$

Sei

$$m_n^* := \sum_{j=1}^n p(j) = \sum_{j=1}^n j^{-s} \quad \text{für alle } n \in \mathbb{N}.$$

Da $s < 1$, gilt

$$(76) \quad m_n^* \rightarrow \infty \quad \text{für } n \rightarrow \infty.$$

Außerdem ist

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{p(n)}{\left(\sum_{j=1}^n p(j) \right)^2} &< C_{30} \sum_{n=1}^{\infty} \frac{n^{-s}}{\left(\int_1^n x^{-s} dx \right)^2} \\ &< C_{31} \sum_{n=1}^{\infty} \frac{n^{-s}}{(n^{1-s})^2} \\ &= C_{31} \sum_{n=1}^{\infty} \frac{1}{n^{2-s}} < \infty, \text{ da } s < 1. \end{aligned}$$

Also gilt

$$(77) \quad \sum_{n=1}^{\infty} \frac{p(n)}{m_n^*} < \infty.$$

Da $(p(n))_{n \in \mathbb{N}}$ eine monoton fallende Nullfolge ist, erhalten wir nach Halberstam und Roth [9], S. 144, Lemma 10 (15)) wegen (76) und (77) für eine Menge $U \subseteq \mathbb{N}$

$$(78) \quad U(n) \sim m_n^* \quad \text{für } n \rightarrow \infty \text{ mit Wahrscheinlichkeit 1.}$$

Weil $U \in E' \cap \bigcap_{\vec{q} \in H_1(h)} E''_{\vec{q}}$ im Beweis von Satz 8 ebenfalls mit Wahrscheinlichkeit 1 gilt, können wir für die dort ausgewählte Menge U auch zusätzlich die Eigenschaft (78) annehmen.

Nun ist

$$\frac{1}{1-s} n^{1-s} - \frac{1}{1-s} = \int_1^n x^{-s} dx < \sum_{j=1}^n n^{-s} = m_n^* < 1 + \int_1^n x^{-s} dx.$$

Es folgt mit (78) nun

$$(79) \quad U(n) \sim \frac{1}{1-s} n^{1-s} \quad \text{für } n \rightarrow \infty.$$

Sei $A = \{a_1, a_2, \dots\} \subseteq \mathbb{N}$, $a_1 < a_2 < \dots$ die in der Voraussetzung von Satz 8 gegebene Menge. Ferner sei

$$U = \{u_1, u_2, \dots\}, \quad u_1 < u_2 < \dots$$

$$\text{und} \quad A^U = \{a_{u_1}, a_{u_2}, \dots\}.$$

Es sei j maximal mit $a_j < n$; dann ist $j = A(n)$.

Es sei m maximal mit $a_{u_m} < n$; dann ist $m = A^U(n)$.

Also ist m maximal mit $u_m < j$ und es gilt $m = U(j)$.

Damit folgt

$$A^U(n) = m = U(j) = U(A(n)).$$

Da im Beweis von Satz 8 die Menge $\tilde{A}$ endlich ist, folgt

¹⁵⁾ In [9] wird für dieses Lemma (in Hypothesis A) noch zusätzlich $p(n) < 1$ für $n=1, 2, \dots$ gefordert (was hier für $n=1$ nicht erfüllt ist). Diese Voraussetzung ist jedoch überflüssig, wie Theorem 11, a.a.O., S. 140 zeigt, aus welchem dieses Lemma folgt.

mit $A' = A^U \cup \tilde{A}$ und mit (79) nun

$$(80) \quad A'(n) \sim A^U(n) = U(A(n)) \sim \frac{1}{1-s} A(n)^{1-s} \quad \text{für } n \rightarrow \infty.$$

Im Beweis von Lemma 18 wurde festgelegt

$$a := \frac{1}{h-1} + c$$

$$b := \frac{1}{h-1} - 2c$$

und im Lemma 25

$$c := \varepsilon \cdot 9^{h-1-h_1}$$

Aus (75) folgt

$$(81) \quad 1-s =: 1-s_h = 1 - \frac{1}{\left(\frac{1}{h-1} + c\right)h} \left(\frac{1}{h-1} - 5c\right) = \frac{1 + (h+5)c}{\frac{h}{h-1} + hc} \\ = \frac{h-1}{h} \cdot \frac{1 + (h+5)c}{1 + (h-1)c}.$$

Wir erhalten damit

$$(82) \quad 1-s_h \longrightarrow \frac{h-1}{h} \quad \text{für } \varepsilon \rightarrow 0.$$

In Lemma 25 ist für $h=3$ zunächst $A=Q$ und $s=s_3$ wie in (81).

Wegen $Q(n) \sim n^{1/2}$ ist nach (80)

$$A_3(n) \sim \frac{1}{1-s_3} n^{\frac{1}{2}(1-s_3)} \quad \text{für } n \rightarrow \infty.$$

Aus (82) folgt

$$C'_{3,\varepsilon} = \frac{1}{1-s_3} \rightarrow \frac{3}{2} \quad \text{für } \varepsilon \rightarrow 0.$$

Für $h=4$, $A=A_3$ und $s=s_4$ wie in (81) erhalten wir unter Beachtung von (80), daß

$$(83) \quad A_4(n) \sim \frac{1}{1-s_4} (A_3(n))^{1-s_4} \sim \frac{1}{1-s_4} \left(\frac{1}{1-s_3} n^{\frac{1}{2}(1-s_3)}\right)^{1-s_4}$$

und

$$(84) \quad C'_{4,\varepsilon} = \frac{1}{1-s_4} \left(\frac{1}{1-s_3}\right)^{1-s_4} \longrightarrow \frac{4}{3} \cdot \left(\frac{3}{2}\right)^{3/4} \quad \text{für } \varepsilon \rightarrow 0.$$

Durch fortgesetzte Anwendung von (80) erhält man, wie behauptet

$$B_{h,\varepsilon}(n) \sim A_h(n) \sim C'_{h,\varepsilon} n^{1/h + \varepsilon'},$$

wobei nach der Ungleichung (32^(h)) im Beweis von Lemma 25 ist $0 < \varepsilon' < \varepsilon$, und für $\varepsilon \rightarrow 0$ gilt wegen (82)

$$C'_{h,\varepsilon} \longrightarrow \prod_{j=3}^h \left(\frac{j}{j-1} \right)^{\prod_{i=j+1}^h \left(\frac{i-1}{i} \right)} = h \sqrt[h]{\frac{h}{4 h!}} < 2,724. \quad 16)$$

Setzt man $h_1=4$, so ist für $h=3$ zunächst $c_3 = \varepsilon \cdot 9^{2-4} = \frac{\varepsilon}{81}$.

Aus (81) folgt

$$1-s_3 = \frac{2}{3} \cdot \frac{1+8/81}{1+2/81}.$$

Für $h=h_1=4$ ist $c_4 = \varepsilon \cdot 9^{3-4} = \frac{\varepsilon}{9}$ und (81) liefert

$$1-s_4 = \frac{3}{4} \cdot \frac{1+\varepsilon}{1+\varepsilon/3}.$$

Damit folgt aus (84) der behauptete Wert für $C'_{4,\varepsilon}$.

Aus (83) erhalten wir

$$\begin{aligned} \frac{1}{4} + \varepsilon' &= \frac{1-s_3}{2} (1-s_4) \\ &= \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{1+8\varepsilon/81}{1+2\varepsilon/81} \cdot \frac{3}{4} \cdot \frac{1+\varepsilon}{1+\varepsilon/3} \end{aligned}$$

Also

$$\begin{aligned} \varepsilon' &= \frac{1}{4} \cdot \left(\frac{243 + 267\varepsilon + 24\varepsilon^2}{243 + 87\varepsilon + 2\varepsilon^2} - 1 \right) \\ &= \frac{\varepsilon}{2} \cdot \frac{90 + 11\varepsilon}{243 + 87\varepsilon + 2\varepsilon^2} < \frac{\varepsilon}{5} \quad \text{für alle } \varepsilon > 0. \end{aligned}$$

¹⁶⁾ Diese obere Schranke erhält man leicht mit Hilfe der Stirlingschen Formel $h! \geq \left(\frac{h}{e}\right)^h \sqrt{2\pi h}$.

A n h a n g

Bemerkungen zu Basenkonstruktionen von Stöhr

Als ein wichtiger Aspekt bei der Beschäftigung mit Basen können deren Minimaleigenschaften angesehen werden, die sich auf unterschiedliche Art und Weise präzisieren lassen. A. Stöhr hat in seiner Arbeit "Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I" [23], S. 51-53 verschiedene Definitionen für Minimalbasen vorgestellt und diskutiert, wobei die Minimalbasen sieben-ter und achter Art (in der dortigen Zählung) von besonderem Interesse sind.

Eine Basis B der Ordnung h heißt Minimalbasis sieben-ter Art, wenn keine echte Teilmenge von B eine Basis der Ordnung h ist.

Eine Basis B der Ordnung h heißt Minimalbasis achter Art, wenn für eine Konstante $C > 0$ und für alle $n \in \mathbb{N}$ gilt

$$B(n) \leq C n^{1/h} .$$

A. Stöhr [21] und D. Raikow [15] haben unabhängig voneinander folgende Minimalbasen A_h achter Art der Ordnung h angegeben:

$$(85) \quad A_h := \bigcup_{k=0}^{h-1} A_h^{(k)}, \text{ wobei } A_h^{(k)} := \left\{ \sum_{j=0}^r e_j 2^{k_2 j h} \mid r \in \mathbb{N}_0, e_j \in \{0, 1\} \right\}$$

Stöhr [22] schätzte deren Anzahlfunktionen nach oben ab durch

$$A_h(n) \leq \frac{2}{e \log 2} h \sqrt{2} h \sqrt{1-2^{-h}} h \sqrt{n} .$$

Die Basen A_h sind meines Wissens die bisher "dünnsten" bekannten Basen. Es läßt sich außerdem leicht zeigen:

Bemerkung. Die Basen A_h in (85) der Ordnung $h \geq 2$ sind Minimalbasen siebenter Art.

Beweis. Aus (85) folgt sofort, daß für $k_1 \neq k_2$, $k_1, k_2 \in \{0, 1, \dots, h-1\}$ gilt $A_h^{(k_1)} \cap A_h^{(k_2)} = \{0\}$. Da für $h \geq 2$ das Element 0 in jeder Basis der Ordnung h enthalten ist, sei nun $0 < a \in A_h$, etwa

$$a = \sum_{j=0}^r e_j(a) 2^{k_2 j h} \in A_h^{(k)} \quad \text{für ein } k \in \{0, 1, \dots, h-1\},$$

wobei wieder $e_j(a) \in \{0, 1\}$ ist. Wir wählen

$$a^{(m)} := \sum_{j=0}^r 2^m 2^{j h} \in A_h^{(m)} \quad \text{für } m=0, 1, \dots, k-1, k+1, \dots, h-1.$$

Es folgt

$$\begin{aligned} (86) \quad n &:= a + \sum_{\substack{m=0 \\ m \neq k}}^{h-1} a^{(m)} \in hA_h \\ &= \sum_{j=0}^r (e_j(a) 2^k + \sum_{\substack{m=0 \\ m \neq k}}^{h-1} 2^m) 2^{j h} =: \sum_{j=0}^r s_j 2^{j h} \end{aligned}$$

Wir zeigen nun, daß n außer (86) keine andere, davon wesentlich verschiedene Darstellung mit h Summanden aus A_h besitzt. Dazu betrachten wir $D_h := \{0, 1, 2, 2^2, \dots, 2^{h-1}\}$ und weisen nach, daß die Zahlen s_j , $j=0, 1, \dots, r$, die als Ziffern im 2^h -System aufgefaßt werden können, als Summe von h Ziffern aus D_h nur auf die obige Weise, also nur durch

$$e_j(a) 2^k + \sum_{\substack{m=0 \\ m \neq k}}^{h-1} 2^m = s_j$$

darstellbar sind und daß Überträge nicht auftreten.

Es sei für $d'_m \in D_h$, $m=0, 1, \dots, h-1$ und für $t \in \mathbb{N}_0$ also

$$e_j(a)2^k + \sum_{\substack{m=0 \\ m \neq k}}^{h-1} 2^m + t \cdot 2^h = s_j + t \cdot 2^h = \sum_{m=0}^{h-1} d'_m ,$$

dann folgt

$$(87) \quad (t+1)2^h - 1 = \sum_{m=0}^{h-1} 2^m + t \cdot 2^h = s_j + t \cdot 2^h + (1 - e_j(a))2^k \\ = \sum_{m=0}^h d_m ,$$

wobei

$$d_m := \begin{cases} d'_m & \text{für } 0 \leq m \leq k-1 \\ 1 - e_j(a) & \text{für } m = k \\ d'_{m-1} & \text{für } k+1 \leq m \leq h \end{cases}$$

und somit $d_m \in D_h$ für $m=0,1,\dots,h$.

Wegen $2 \nmid (t+1)2^h - 1$ ist $d_m = 1$ für ein m , wobei o.B.d.A.

dieses $m=0$ sei. Also

$$(t+1)2^h - 2 = \sum_{m=1}^h d_m .$$

Für $m' \in \mathbb{N}$, $m' \leq h-1$ sei bereits gezeigt, daß

$$d_0 = 1, d_1 = 2, d_2 = 2^2, \dots, d_{m'-1} = 2^{m'-1}$$

und

$$(t+1)2^h - 2^{m'} = \sum_{m=m'+1}^h d_m .$$

Wegen $2^{m'} \mid (t+1)2^h - 2^{m'}$ und $2^{m'+1} \nmid (t+1)2^h - 2^{m'}$ gilt daher für ein m , daß $d_m = 2^{m'}$, wobei o.B.d.A. $m=m'$ sei. Es folgt

$$(t+1)2^h - 2^{m'+1} = \sum_{m=m'+1}^h d_m .$$

Nach insgesamt $h-1$ Schritten folgt $d_m = 2^m$ für $m=0,1,\dots,h-1$, also $t \cdot 2^h = d_h \leq 2^{h-1}$. Damit gilt $t = d_h = 0$, d.h. es erfolgt kein Übertrag. Wir erhalten aus (87) nun

$$s_j = s_j + t \cdot 2^h = \sum_{\substack{m=0 \\ m \neq k}}^h d_m + e_j(a)2^k = \sum_{\substack{m=0 \\ m \neq k}}^{h-1} 2^m + e_j(a)2^k$$

als einzige Darstellung von s_j mit h Summanden aus D_h , da

auch $e_j(a)2^k \in D_h$ ist.

Da in einer beliebigen Darstellung von n durch h Summanden aus A_h jeder dieser Summanden in einer Menge $A_h^{(m)}$ liegt und daher im 2^h -System nur Ziffern aus $\{0, 2^m\}$ besitzt, ist die Darstellung (86) - bis auf Reihenfolge der Summanden - die einzige. Damit ist $A_h \setminus \{a\}$ keine Basis der Ordnung h . Das gilt für jedes $a \in A_h$. Also ist A_h Minimalbasis der Ordnung h von siebenter Art ■

Im Anschluß an die oben erwähnte Diskussion der verschiedenen Arten von Minimalbasen stellt Stöhr in [23], S. 53-57 eine Klasse von Basen vor, die er rekurrente Basen nennt.

Für $h \in \mathbb{N}_0$ und $M \in \mathbb{N}_0$, $|M| < \infty$ sei

$$N(h, M) := \min \{ n \in \mathbb{N} \mid n \notin hM \} .$$

Sei $k \in \mathbb{N}$ und

$$B^{(0)} := A_k = \{a_0, a_1, a_2, \dots, a_k\} \subseteq \mathbb{N}_0 \quad \text{mit} \\ a_0 = 0 < a_1 = 1 < a_2 < \dots < a_k .$$

Wir definieren für $j \in \mathbb{N}$ die Mengen $B^{(j)}$ rekursiv durch

$$B^{(j)} := B^{(j-1)} \cup \{N(h, B^{(j-1)})\} .$$

Offenbar ist

$$B := \bigcup_{j=0}^{\infty} B^{(j)}$$

eine Basis der Ordnung h und heißt die zu A_k gehörende rekurrente Basis der Ordnung h .

Eine rekurrente Basis B heißt periodisch, falls es ein $s \in \mathbb{N}_0$ und ein $q \in \mathbb{N}$ gibt mit folgender Eigenschaft: Für alle $n \in \mathbb{N}$, $n \geq s$ gilt $n \in B$ genau dann, wenn $n+q \in B$.

Für jedes Element $b \in B$ mit $b > a_k$ einer zu A_k gehörenden rekurrenten Basis B ist $B \setminus \{b\}$ keine Basis der Ordnung h . Daher erhalten wir durch Weglassen von gewissen Elementen $b \leq a_k$ eine Minimalbasis siebenter Art, falls B nicht selbst schon eine solche ist. Dennoch gilt für rekurrente Basen B sehr oft $B(n) > Cn$ für alle $n \in \mathbb{N}$, da sich die meisten untersuchten rekurrenten Basen als periodisch erwiesen haben. Im Hinblick auf das Interesse an "dünnen" Basen stellte Stöhr [23] folgende Fragen:

Gibt es ein h und eine endliche Menge A_k so, daß die zugehörige rekurrente Basis nicht periodisch ist?

Falls das zu bejahen ist, gibt es rekurrente Basen, die Minimalbasen achter Art sind?

Keine der beiden Fragen konnte bisher beantwortet werden. Im folgenden wird lediglich gezeigt, daß bei beliebig vorgegebenem A_k und bei genügend großem h die zugehörige rekurrente Basis periodisch ist.

Seien $h_0 = h_0(A_k)$ und $h_1 = h_1(A_k)$ natürliche Zahlen, die wie folgt definiert sind:

h_0 ist minimal mit der Eigenschaft, daß für alle $h \in \mathbb{N}$, $h > h_0$ gilt

$$N(h, A_k) > a_k.$$

h_1 ist minimal mit der Eigenschaft, daß für alle $h \in \mathbb{N}$, $h > h_1$ gilt

$$(88) \quad N(h+1, A_k) = N(h, A_k) + a_k.$$

(Zur Existenz von h_1 siehe etwa Rødseth [16], S. 170-171)

Wegen $N(h_0-1, A_k) \leq a_k$ kann $h = h_0-1$ die Gleichung (88) nicht

erfüllen. Es folgt

$$(89) \quad h_1 \geq h_0 - 1.$$

Auf E. Selmer [18] gehen folgende Bezeichnungen zurück:

Ist $h \geq h_0(A_k)$, so gilt für die Elemente der zu A_k gehörenden rekurrenten Basis B der Ordnung h , daß

$$a_0 = 0 < a_1 = 1 < a_2 < \dots < a_k < N(h, A_k) = N(h, B^{(0)}) < N(h, B^{(1)}) < \dots$$

In diesem Falle sei für $j=1, 2, \dots$

$$a_{k+j} := N(h, B^{(j-1)}),$$

$$A_{k+j} := B^{(j)} = \{a_0, a_1, \dots, a_k, a_{k+1}, \dots, a_{k+j}\},$$

$$d_j := a_{k+j} - a_{k+j-1}.$$

Ist B periodisch und gilt $d_j = d_1$ für $j=1, 2, \dots$, so heißt

B rein-1-periodisch.

Sei $n \in \mathbb{N}$ und $h' \in \mathbb{N}_0$. Eine Darstellung von n mit h' Summanden aus B bezeichnen wir als h' -Darstellung von n .

Selmer hat in [18] u.a. für $k=3$ zu allen Mengen $A_k = A_3$ und allen $h \geq h_0(A_3)$ sämtliche rekurrenten Basen der Ordnung h bestimmt, die rein-1-periodisch sind.

Hier beweisen wir zunächst eine Verallgemeinerung eines Satzes von Selmer [18] (Theorem 1).

Satz 10. Sei $A_k = \{a_0, a_1, a_2, \dots, a_k\} \subseteq \mathbb{N}_0$, $a_0 = 0 < a_1 = 1 < a_2 < \dots < a_k$ und $h \in \mathbb{N}$, $h \geq h_0$. Es sei B die zu A_k gehörende rekurrente Basis der Ordnung h .

Wir setzen voraus, daß jede natürliche Zahl in $[a_{k+1}, a_{k+1} + d_1[$ eine h -Darstellung besitzt, in welcher a_k oder a_{k+1} als Summand auftritt.

Dann sind die beiden folgenden Aussagen äquivalent:

(i) B ist rein-1-periodisch.

(ii) $a_k + td_1 \notin hA_k$ für $t=2,3,\dots$.

Beweis. (i) $\Rightarrow$ (ii): Da B rein-1-periodisch ist, folgt

$$a_k + td_1 = a_{k+t} = N(h, A_{k+t-1}) \notin hA_k \text{ für } t=1,2,\dots$$

(ii) $\Rightarrow$ (i): Durch Induktion nach t zeigen wir für alle $t \in \mathbb{N}_0$, daß

$$(90) \quad a_{k+t} = a_k + td_1.$$

Für $t=0$ ist (90) trivial; für $t=1$ gilt (90) nach Definition von d_1 .

Wir nehmen an, (90) gelte für $t \in \mathbb{N}$ und alle kleineren Indizes.

Nach Induktionsvoraussetzung für $t \in \mathbb{N}$ ist

$$a_{k+t} = a_k + td_1 = a_{k+1} + (t-1)d_1.$$

Sei $n \in [a_{k+t}, a_{k+t} + d_1[\cap \mathbb{N}$, dann folgt

$n - (t-1)d_1 \in [a_{k+1}, a_{k+1} + d_1[\cap \mathbb{N}$. Nach Voraussetzung folgt

$$(91) \quad n - (t-1)d_1 = a_1 + \sum_{i=1}^{h-1} a^{(i)} \text{ mit } a_1 \in \{a_k, a_{k+1}\}, a^{(i)} \in B.$$

Es gilt sogar

$$a^{(i)} \in A_{k+1} \text{ für } i=1,2,\dots,h-1,$$

denn $a_{k+2} = N(h, A_{k+1})$ hat keine h -Darstellung mit Elementen, die kleiner als a_{k+2} sind, so daß mit nochmaliger

Beachtung der Voraussetzung $a_{k+2} \notin [a_{k+1}, a_{k+1} + d_1[$ folgt,

also wegen $a_{k+2} > a_{k+1}$ auch $a_{k+2} \geq a_{k+1} + d_1 > n - (t-1)d_1 > a^{(i)}$.

Damit ist $a^{(i)} \in A_{k+1}$ für $i=1,2,\dots,h-1$.

Aus (91) folgt $n = a_1 + (t-1)d_1 + \sum_{i=1}^{h-1} a^{(i)}$, wobei nach In-

dukionsvoraussetzung für $t-1$ und t gilt, daß

$$a_1 + (t-1)d_1 \in [a_{k+t-1}, a_{k+t}).$$

Also ist

$$(92) \quad [a_{k+t}, a_{k+t} + d_1] \cap \mathbb{N} \subseteq hA_{k+t}.$$

Annahme: $a_{k+t} + d_1 = \sum_{i=1}^h b^{(i)}$, $b^{(i)} \in A_{k+t}$ für $i=1, 2, \dots, h$.

Es sei $b^{(h)}$ das größte Element von $b^{(1)}, b^{(2)}, \dots, b^{(h)}$.

Wir machen die weitere

Annahme: $b^{(h)} = a_{k+j}$ für ein j mit $1 \leq j \leq t$.

Unter Beachtung der Induktionsvoraussetzung würde folgen

$$a_{k+t} + d_1 = a_{k+j} + \sum_{i=1}^{h-1} b^{(i)} = a_{k+j-1} + d_1 + \sum_{i=1}^{h-1} b^{(i)}.$$

Dann hätten wir

$$a_{k+t} = a_{k+j-1} + \sum_{i=1}^{h-1} b^{(i)}.$$

Wegen $a_{k+t} > a_{k+j-1} > 0$ wären alle h Summanden auf der rechten Seite der letzten Gleichung kleiner als a_{k+t} , was wegen $a_{k+t} = N(h, A_{k+t-1})$ unmöglich ist.

Also ist $b^{(i)} \leq b^{(h)} \leq a_k$ für $i=1, 2, \dots, h$, woraus nach der ersten Annahme folgt

$$a_k + (t+1)d_1 = a_{k+t} + d_1 \in hA_k.$$

Das widerspricht aber (ii). Also ist auch die erste Annahme falsch und es gilt

$$a_{k+t} + d_1 \notin hA_{k+t}.$$

Mit (92) folgt daraus, daß (90) für $t+1$ gilt:

$$a_k + (t+1)d_1 = a_{k+t} + d_1 = N(h, A_{k+t}) = a_{k+t+1}.$$

Wegen (90) ist B rein-1-periodisch ■

Als Folgerung des soeben bewiesenen Satzes ergibt sich die Periodizität rekurrenter Basen bei genügend großen h . Diese Aussage hat der Verfasser ursprünglich anders be-

wiesen. Der Schlußteil des hier dargestellten Beweises geht im wesentlichen auf E. Selmer [18] zurück.

Folgerung. Sei $A_k = \{a_0, a_1, a_2, \dots, a_k\} \subseteq \mathbb{N}_0$, $a_0 = 0 < a_1 = 1 < a_2 < \dots < a_k$ und

$$(93) \quad h \geq 2 \frac{(a_k-1)(a_k-k)}{a_k - a_{k-1}} + 3$$

Dann ist die zu A_k gehörende rekurrente Basis B der Ordnung h rein-1-periodisch.

Beweis. Nach Rødseth [16], S. 173 ist

$$h_1 = h_1(A_k) \leq \left\lceil \frac{(a_k-1)(a_k-k) - 1}{a_k - a_{k-1}} \right\rceil \quad \text{für } a_k > k > 2.$$

Im Fall $a_k = k$ (und damit auch für $k=1$) gilt nach Definition von h_1 , daß $h_1 = 1$ und im Fall $a_k \neq k=2$, daß $h_1 = a_k - 2 = a_k - k$ ist (siehe Rødseth [16], S. 166). Damit hat man für alle $A_k \subseteq \mathbb{N}_0$, $0, 1 \in A_k$, daß

$$h_1 \leq \frac{(a_k-1)(a_k-k)}{a_k - a_{k-1}} + 1.$$

Wegen (93) gilt dann

$$(94) \quad h \geq 2h_1 + 1.$$

Da $h_0 > 1$ ist, folgt aus (94) und (89), daß

$$h \geq 2(h_0 - 1) + 1 \geq h_0 - 1 + 1 = h_0, \quad \text{also} \\ h \geq h_0.$$

Wegen (94) ist $h > h_1$, also gilt nach (88), daß

$$[0, d_1[= [0, N(h, A_k) - a_k[= [0, N(h-1, A_k)[.$$

Folglich besitzt jedes $n \in [0, d_1[\cap \mathbb{N}$ eine $(h-1)$ -Darstellung und jedes $n \in [a_{k+1}, a_{k+1} + d_1[\cap \mathbb{N}$ eine h -Darstellung mit a_{k+1} als Summand. Damit sind die Generalvoraussetzungen von Satz 10 erfüllt.

Aus (94) folgt

$$2h - 2h_1 - 1 \geq h .$$

Ferner ist wegen (88) und $h \geq h_1$ noch

$$N(h, A_k) = N(h_1, A_k) + (h - h_1)a_k .$$

Damit erhält man für $t \geq 2$, daß

$$\begin{aligned} a_k + td_1 &\geq a_k + 2d_1 = a_k + 2N(h, A_k) - 2a_k \\ &= 2N(h_1, A_k) + (2h - 2h_1 - 1)a_k > ha_k . \end{aligned}$$

Also ist $a_k + td_1 \notin hA_k$ und wir erhalten mit Satz 10 die
Behauptung ■

Zusammenfassung

Sei Q_0 die Menge der Quadrate der nicht-negativen ganzen Zahlen. Zunächst wird in § 2 gezeigt (Satz 1), daß $Q_0 \setminus \{n^2\}$ Basis der Ordnung 4 ist genau dann, wenn $n \neq 0, 5, 2^k$ und $3 \cdot 2^k$ ($k \in \mathbb{N}_0$).

Das Hauptresultat in § 3 ist folgendes: Sei $4 \leq h \in \mathbb{N}$ und $\varepsilon > 0$, dann gibt es Basen $B_{h,\varepsilon} \subseteq Q_0$ der Ordnung h , so daß $B_{h,\varepsilon}(n) = O(n^{1/h+\varepsilon})$. Für $h=4$ werden damit Vermutungen von Erdős und Nathanson [7] und Choi, Erdős und Nathanson [2] bewiesen (Sätze 4,5 und 9). Außerdem wird gezeigt (in 3.10), daß für ein ε' mit $0 < \varepsilon' < \varepsilon$ gilt $B_{h,\varepsilon}(n) \sim C'_{h,\varepsilon} n^{1/h+\varepsilon'}$ für $n \rightarrow \infty$. Bei festem h gilt

$$C'_{h,\varepsilon} \rightarrow h \sqrt[h]{\frac{h}{4h!}} < 2,724 \quad \text{für } \varepsilon \rightarrow 0.$$

Im Anhang werden spezielle Basen von A. Stöhr betrachtet. Es wird u.a. gezeigt, daß die von ihm in [17] eingeführten rekurrenten Basen der Ordnung h bei beliebiger endlicher Startmenge periodisch sind, falls h genügend groß ist (s. Folgerung aus Satz 10).

L i t e r a t u r v e r z e i c h n i s

- [1] P.T. Bateman, On the representations of a number as the sum of three squares, Trans. Amer. Math. Soc. 71 (1951), S. 70-101
- [2] S.L.G. Choi, P. Erdős und M.B. Nathanson, Lagrange's theorem with $N^{1/3}$ squares, Proc. Amer. Math. Soc. 79 (1980), S. 203-205
- [3] E. Deinert, E. Härtter und J. Zöllner, Verzichtbare und unverzichtbare Elemente bei der Darstellung als Summe und als Differenz von Quadraten, Acta Arith. 45 (1985), S. 71-79
- [4] L.E. Dickson, Introduction to the theory of numbers, New York, 1957
- [5] P. Erdős, Problems and results in additive number theory, Colloque sur la Théorie des Nombres (Brüssel, 1956), S. 127-137
- [6] P. Erdős und M.B. Nathanson, Lagrange's theorem in thin subsequences of squares, in: I. Gani und V.K. Rohatgi (Hrsg.), Contributions to probability, New York, 1981, S. 3-9
- [7] P. Erdős und M.B. Nathanson, Systems of distinct representations and minimal bases in additive number theory, Lecture Notes in Math. 751 (1979), S. 89-107
- [8] P. Erdős und A. Rényi, Additive properties of random sequences of integers, Acta Arith. 6 (1960), S. 83-110
- [9] H. Halberstam und F.K. Roth, Sequences, Vol. I, London und New York, 1966
- [10] G.H. Hardy und E.M. Wright, An Introduction to the theory of numbers, Oxford, 1954
- [11] E. Härtter und J. Zöllner, Darstellungen natürlicher Zahlen als Summe und Differenz von Quadraten, Det Kgl. Norske Vidensk. Selk. Skr., 1977 No.1, S. 1-8

- [12] E. Landau, Vorlesungen über Zahlentheorie, Aus der elementaren Zahlentheorie, New York, 1950
- [13] M.B. Nathanson, Waring's problem for sets of density zero, Lecture Notes in Math. 899 (1981), S. 301-310
- [14] G. Pall, On sums of squares, Amer. Math. Monthly 40 (1933), S. 10-18
- [15] D. Raikow, Über Basen der natürlichen Zahlenreihe (russ. u. deutsch.), Mat. Sbornik N.S. 2 (1937), S. 595-597
- [16] Ø. Rødseth, On h-bases for n , Math. Scand. 48 (1981), S. 165-183
- [17] E.S. Selmer, Some h-bases for n related to Waring's problem, Department of Pure Math., Universität Bergen, Norwegen, 1983
- [18] E.S. Selmer, On a problem of Stöhr, Department of Pure Math., Universität Bergen, Norwegen, 1984
- [19] C.L. Siegel, Über die Klassenzahl quadratischer Zahlkörper, Acta Arith. 1 (1935), S. 83-86
- [20] W. Sierpiński, Elementary theory of numbers, Warschau, 1964
- [21] A. Stöhr, Eine Basis h -ter Ordnung für die Menge der natürlichen Zahlen, Math. Zeitschr. 42 (1937), S. 739-743
- [22] A. Stöhr, Anzahlabschätzung einer bekannten Basis h -ter Ordnung, Math. Zeitschr. 47 (1942), S. 778-787; 48 (1942/43), S. 792
- [23] A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, J. reine angew. 194 (1955), S. 40-65
- [24] J. Zöllner, Über Mengen natürlicher Zahlen, für die jede euklidische Darstellung eine minimale Koeffizientensumme besitzt, Diplomarbeit, Mainz 1974
- [25] J. Zöllner, Über eine Vermutung von Choi, Erdős und Nathanson, Acta Arith. 45 (1985), S.

Lebenslauf

Als Sohn des Maurers Paul Zöllner und dessen Ehefrau Gertrud geb. Schmidt wurde ich am 13. Dez. 1942 in Radeberg, Kreis Dresden, geboren. Mein Vater fiel 1945 als Volksturmssoldat. Nach Besuch der Volksschulen ab Herbst 1949 in Radeberg und von Okt. 51 bis April 58 in Neuwied begann ich im Juni 58 eine Lehre als Stahlbauschlosser, die ich im April 61 mit der Facharbeiterprüfung abschloß. Es folgten einige Jahre (1961-67) beruflicher Tätigkeit. Während dieser Zeit erwarb ich in einer Berufsaufbauschule in Teilzeitform in Neuwied die Fachschulreife. Ab April 67 besuchte ich das Koblenz-Kolleg, wo ich im Sept. 69 die allgemeine Hochschulreife erlangte. Vom WS 69/70 bis WS 76/77 studierte ich an der Johannes Gutenberg-Universität in Mainz mit einem Stipendium der Studienstiftung des deutschen Volkes Mathematik im Hauptfach und Physik im Nebenfach und legte im Feb. 1975 die Diplomprüfung ab. Von Feb. 77 bis Juli 78 wurde ich am Studienseminar Mainz für das Lehramt an Gymnasien in Mathematik und Physik ausgebildet. Nach dem zweiten Staatsexamen im Juni 78 unterrichtete ich in diesen Fächern bis Juli 81 am Gutenberg-Gymnasium in Mainz und nebenamtlich bis Jan. 82 am Studienkolleg. Seit Feb. 82 bin ich wissenschaftlicher Mitarbeiter am Fachbereich Mathematik der Universität Mainz, was mir durch eine Beurlaubung vom Staatsdienst ermöglicht wurde.

Joachim Zöllner
Wallaustr. 77

Staatszugehörigkeit: deutsch

6500 Mainz

